August 2019

Bitco
A Peer-to-Peer Electronic Cash Syst
Satoshi Nakamoto
Bitcoin Cash (BCH) Wallet
4.68168026 BCH

Cryptocurrency: A Primer for Policy-Makers

Zack Gold and Megan McBride

CRM-2019-U-020185-Final

Abstract

This primer is an effort to address a gap in knowledge about cryptocurrencies and the cryptocurrency ecosystem among the policymaking community and advance the understanding of cryptocurrencies and consideration of their national security implications. Cryptocurrencies are strictly digital currencies, are typically overseen by a decentralized peer-to-peer community, and are secured through cryptography. We use clear, non-technical language to describe complex concepts and demystify overly technical terms in order to explain the technical and economic aspects of cryptocurrency, why they are used, and the benefits and drawbacks to cryptocurrencies compared to conventional currencies—like the US dollar. We conclude by considering some cryptocurrency-related issues of which greater exploration would benefit US national security.

This document contains the best opinion of CNA at the time of issue.

It does not necessarily represent the opinion of the sponsor or client.

Distribution

Approved for public release. Unlimited distribution.

Cover image credit: "Photo of a mobile phone with a Bitcoin Cash wallet, Bitcoin whitepaper by Satoshi Nakamoto and Bitcoin.com pen." BitcoinXio, Apr. 15, 2018.

Approved by: **August 2019**

Jonathan Schroden, Research Program Director
Special Operations Program
Center for Stability & Development
Strategy, Policy, Plans, and Programs Division (SP3)

Request additional copies of this document through inquiries@cna.org.

Executive Summary

In 2017, the value of one Bitcoin skyrocketed to more than $20,000. Media coverage increased, and even people who did not join the investment frenzy became aware of so-called "cryptocurrencies." Despite this familiarity, few actually understand cryptocurrencies and the implications they may have on US interests, from global finance to national security to good governance.

Cryptocurrencies are strictly digital currencies (and not merely the digital exchange of conventional currencies such as US dollars), are typically overseen by a decentralized peer-to-peer community, and are secured through cryptography. Cryptocurrency supporters highlight the potential for cryptocurrencies to improve buyer-seller transactions. Meanwhile, news reports over the past decade have raised red flags about the use of this technology by criminals, terrorists, and rogue states.

CNA initiated this study to explore the implications of cryptocurrencies for special operations forces (SOF), the broader US Department of Defense (DOD), and other US government agencies. In the process of considering national security implications, we found a gap in knowledge about cryptocurrencies and the cryptocurrency ecosystem among the policy-making community. This primer is an effort to address that gap and advance the understanding of cryptocurrencies and consideration of their national security implications.

Cryptocurrencies differ from most conventional currencies in five significant ways:

1. Cryptocurrencies are not controlled or regulated by banks or governments.
2. Cryptocurrencies rely on a decentralized system (known as the "blockchain").
3. Cryptocurrency exchange rates can be extremely volatile.
4. Cryptocurrencies typically have longer transaction times.
5. Cryptocurrency transactions are pseudonymous[1] or anonymous.

[1] The individual conducting the transaction is known, but his or her true identity may be unknown.

Figure: What is a blockchain?

*A **blockchain** is an immutable decentralized ledger:*

- *Immutable* — each new block essentially locks in previous blocks
- *Decentralized* — a peer-to-peer network of computerized contributors creates new blocks
- *Ledger* — a list (i.e., a chain) of individual records (i.e., blocks)

For more information on blockchains, see the section "Cryptocurrencies as technology."

Source: CNA.

Cryptocurrencies (Bitcoin being the first and most popular) were developed to solve the problem of buyers cheating sellers (through a currency problem called "double-spending") without introducing someone to oversee the transaction (a third-party authority). Bitcoin's creators addressed this issue through cryptographic problem-solving (called "mining") conducted by a decentralized, computerized network.

Cryptocurrency use is still far from mainstream, but using cryptocurrencies for transactions has potential benefits. First, cryptocurrencies provide secure transactions without needing to place trust in the third-party authority of banks. Second, cryptocurrencies can be accepted globally, so goods and services could be purchased anywhere in the world without having to first exchange payment into local currency. Third, similar to cash purchases, cryptocurrency transactions do not require participants to provide identification; however, moving large sums of cryptocurrencies is much easier than moving bulk cash. Fourth, unlike brick-and-mortar banks and exchange houses—where cash transactions take place—cryptocurrency transactions are processed around the clock.

However, cryptocurrencies also suffer from weaknesses. Some vulnerabilities are built into the very systems of cryptocurrency and the blockchain, such as exchange rate volatility, lengthy transaction times, and the potential that the system could be hijacked. Additionally, hackers have stolen cryptocurrencies numerous times.

It is worth keeping in mind that the relative benefits of cryptocurrencies over conventional currencies increase in developing and under-developed countries and in nations with poor fiscal and monetary management. For example, if local conventional currencies suffer from high exchange rate volatility, the swings of cryptocurrency values may be less concerning.

Using cryptocurrencies also has relative benefits for those who engage in illicit activity. In our companion paper, we explore cryptocurrency issues for SOF. Although written with a SOF audience in mind, that report may also be of interest to a broader policy audience because it includes: (1) a detailed taxonomy and examples of nefarious activities involving cryptocurrencies, such as funding terrorist activity, money laundering, cybercrimes, and regulatory crimes; (2) a discussion of state-actor engagement in the cryptocurrency arena that explores Iranian, North Korean, Russian, and Venezuelan activity in skirting sanctions, mining cryptocurrencies, participating in exchange hacking and ransomware, and using cryptocurrencies to fund information operations; and (3) analysis attempting to anticipate the mid-term future of the cryptocurrency ecosystem.

Our companion paper ends by highlighting the tactical and strategic challenges and opportunities of cryptocurrencies for SOF. Written for a broader audience, this primer concludes by considering some other cryptocurrency-related issues of which greater exploration would benefit US national security.

These areas include the following challenges:

- **Safe havens for illicit actors.** Transnational criminal organizations and other illicit actors can take advantage of gaps in international regulations of cryptocurrencies to operate freely in countries with lax oversight.
- **Sanctions evasion.** Internationally sanctioned regimes, such as North Korea, purchase, mine, or steal cryptocurrencies to raise funds. Venezuela attempted to access foreign investment by launching its own cryptocurrency, the *petro*.
- **Speed of technological adaptation.** The adoption of new and constantly evolving cryptocurrency technologies can hinder efforts developed by law enforcement and the intelligence community to track illicit activity.

And opportunities:

- **Protection of free speech.** Actors can use cryptocurrencies to raise funds and spread their message outside traditional internet platforms and services (e.g., when the internet is government or private-industry censored).
- **Good governance.** Just as the blockchain secures a cryptocurrency, it has the potential to secure and legitimize functions of governance.

Cryptocurrencies and the technologies related to them are innovative financial tools with implications for national security. We hope this paper—in which we use clear, non-technical language to describe complex concepts and demystify overly technical terms—will help the US government more effectively support legitimate cryptocurrency users and counter illicit ones.

This page intentionally left blank.

Contents

Introduction

In 2017, the value of one Bitcoin skyrocketed to more than $20,000. During that boom, millions of people around the world joined the virtual gold rush by investing in Bitcoin (the first and most popular cryptocurrency), competitor cryptocurrencies, or the blockchain technology underlying the innovation. Media coverage increased, and even people who did not join the frenzy heard the words “Bitcoin,” “cryptocurrencies,” and “blockchain.” In fact, awareness of Bitcoin has risen rapidly since its 2008 launch. By 2018, nearly 80 percent of Americans reported having heard the term “Bitcoin.”[1] Despite this familiarity, few actually understand these technologies and the implications they may have on US interests, from global finance to national security to good governance.

The US Department of Defense (DOD), like the general public, is aware of cryptocurrencies but still lacks a thorough understanding. To fill this knowledge gap, in May 2018, the Joint Special Operations University (JSOU) asked for research on the topic, “The evolution of cryptocurrency: Future challenges and opportunities for SOF” (special operations forces).[2] CNA initiated this study to explore the cryptocurrency ecosystem and help SOF consider the implications of cryptocurrencies on SOF missions, including counter-threat finance.

In the process of researching and writing *Cryptocurrency: Implications for Special Operations Forces*, which we published concurrently with this paper, we realized that—with the exception of some pockets of expertise—few US military and government personnel were working in the field of cryptocurrencies. Indeed, we identified a gap in knowledge of cryptocurrencies among the US policy and decision-making community. We recognized that a simple primer aimed at a national security policy audience would be of value and produced this paper accordingly.

A cryptocurrency expert will find this primer simplistic: that was our intention. Our goal was to explain key cryptocurrency terms, technologies, and applications in easy-to-follow

[1] Nikhilesh De, “Survey: Nearly 80% of Americans Have Heard of Bitcoin,” *Coindesk*, Sept. 6, 2018, https://www.coindesk.com/survey-nearly-80-of-americans-have-heard-of-bitcoin.

[2] Joint Special Operations University, *Special Operations Research Topics 2018 (Revised Edition for Academic Year 2019)*, (MacDill AFB, FL: JSOU Press, 2018), https://jsou.libguides.com/ld.php?content_id=41898487.

language—with many figures and examples. What makes our primer different from the dozens of cryptocurrency explainers on the internet is our attention to issues with policy and national security implications.

This primer does not attempt to explain comprehensively the nuanced intricacies of cryptocurrencies in technical and financial detail. Nor does it explore the far-reaching potential implications of blockchain technology, one of which—logistics—is discussed in CNA's 2018 occasional paper, "Leveraging Blockchain to Secure Logistics Information."[3] Instead, we explain the core issues that are necessary to understand the basics of cryptocurrency (in terms of technology and economics).

The rest of this primer is organized into three main sections. The first section provides a brief history of cryptocurrencies and the problems inherent in digital currencies (indeed, in all currencies) that cryptography aspires to solve. The second section, which makes up the bulk of the primer, explains how cryptocurrencies work. We discuss the technology of cryptocurrencies; the difference between cryptocurrencies and conventional currencies; and how users obtain, hold, and exchange cryptocurrencies. The third section recommends areas in which more research and analysis are required on the impact of cryptocurrencies. These issues should be considered in addition to the cryptocurrency implications for SOF, which we explore in our companion report. Our goal is that this primer will contribute to the understanding of cryptocurrencies among the policy-making community and build knowledge of the implications of this innovative technology on US national security.

Readers that already understand the basics of cryptocurrencies or that are interested in the impact of cryptocurrency on national security are encouraged to read our companion paper. Although written with a SOF audience in mind, that report highlights examples of states and non-state actors using cryptocurrencies for nefarious purposes, which may be of interest to a broader policy audience. *Cryptocurrency: Implications for Special Operations Forces* includes the following: (1) a detailed taxonomy and examples of nefarious activities using cryptocurrencies, such as funding terrorist activity, money laundering, cybercrimes, and regulatory crimes; (2) a discussion of state-actor engagement in the cryptocurrency arena that explores Iranian, North Korean, Russian, and Venezuelan activity in skirting sanctions, mining cryptocurrencies, participating in exchange hacking and ransomware, and using cryptocurrencies to fund information operations; (3) analysis attempting to anticipate the mid-term future of the cryptocurrency ecosystem; and (4) the tactical and strategic challenges and opportunities of cryptocurrencies for SOF.

[3] S. John Spey, *Leveraging Blockchain to Secure Logistics Information*, CNA, 2018, DOP-2018-U-018289-Final.

What Are Cryptocurrencies?

A cryptocurrency is (1) a strictly digital currency (i.e., not a digital exchange of conventional currencies, such as US dollars), (2) typically decentralized, and (3) secured with cryptographic methods. Ideally a cryptocurrency should function as a conventional currency (facilitating the exchange of goods and services), but it should do so in a public, transparent, and secure way.[4] "Virtual currencies" and "virtual assets" are other terms to describe cryptocurrencies.

Figure 1. Conventional currencies

> *We use the phrase* ***conventional currencies*** *to refer to fiat currencies, which are currencies backed by the governments that issue them. Importantly, this type of currency is not tied to a physical good. The linen of a US dollar itself has no intrinsic value. The value of the US dollar is not tied to an intrinsically valuable commodity (such as gold), and the US dollar cannot be exchanged for gold at a fixed rate (as was the case when the US used the gold standard).*

Source: CNA.

Cryptocurrencies differ from most conventional currencies (Figure 1) in five significant ways:

1. Cryptocurrencies are not controlled or regulated by a formal third-party authority (e.g., a bank or government).[5]

[4] In March 2018, Merriam-Webster added "cryptocurrency" to its dictionary, noting that that the word had first been used in 1990 and that a "cryptocurrency" has three core characteristics: "Any form of currency that exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions." Source: Merriam-Webster, "Cryptocurrency," Merriam-Webster website, accessed May 2, 2019, https://www.merriam-webster.com/dictionary/cryptocurrency.

[5] Matthew Frankel, "What is Bitcoin?" *Motley Fool*, Jan. 10, 2017, https://www.fool.com/retirement/2017/01/10/what-is-bitcoin-2.aspx.

2. Cryptocurrencies rely on a decentralized public ledger (known as the "blockchain") instead of a centralized private ledger (a system known as "third-party trust").[6]
3. Cryptocurrency exchange rates can be extremely volatile, depending on supply and demand.
4. Cryptocurrencies typically have longer transaction times than conventional currencies.
5. Cryptocurrency transactions are pseudonymous[7] or anonymous.[8]

We explore these five characteristics further in the "How Do Cryptocurrencies Work?" and "An Assessment of Cryptocurrencies: Weaknesses and Common Myths" sections of this paper. First, we discuss the creation of cryptocurrencies and the problems they were designed to solve.

Why were cryptocurrencies created?

Cryptocurrencies were created to solve the problem of double-spending without relying on trusted third parties, such as governments and central banks. The idea of Bitcoin originated with a loosely affiliated group—known as Cypherpunks—committed to using cryptography as a means to secure privacy.[9] As noted in "A Cypherpunk's Manifesto":

> Privacy in an open society requires anonymous transaction systems....Privacy in an open society also requires cryptography....We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence....We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place....We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography,

[6] Chris Stead, "Bitcoin 101: What Is It and Why Does It Matter?" *IGN*, Jan. 17, 2018, https://www.ign.com/articles/2018/01/17/bitcoin-101-what-is-it-and-why-does-it-matter.

[7] The individual conducting the transaction is known, but his or her true identity may be unknown.

[8] Lucas Nuzzi, "ZEC: Unmatched Privacy in a Public Blockchain," *Medium*, Sept. 17, 2018, https://medium.com/digitalassetresearch/zec-best-in-class-privacy-in-a-public-blockchain-1df2a3728739.

[9] Adrian Chen, "We Need to Know Who Satoshi Nakamoto Is," *The New Yorker*, May 9, 2016, https://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is.

> with anonymous mail forwarding systems, with digital signatures, and with electronic money.[10]

In other words, founders and early adopters of cryptocurrencies were motivated by the idea that government-backed conventional currencies would never guarantee privacy, and they sought a method of global financial transactions outside traditional government-backed systems.[11]

Double-spending

Double-spending is the act of spending a single unit of currency twice, and it is one of the core challenges in the world of currency exchange. Double-spending can occur with any currency and at any time, but it is more likely to occur if the act is easy to hide and low risk.[12]

When currency is physically exchanged, the likelihood of double-spending is incredibly low. It is hard to imagine an easy deception or low-risk means for one person to spend the same $10 bill twice. Double-spending is more likely to happen, however, when currencies are exchanged *digitally.* Clearly, the risks are lower and deception is easier when one person simply promises the same $10 to two online vendors.

The widespread solution to prevent double-spending when *conventional* currencies are exchanged *digitally* is the maintenance of a centralized ledger by a recognized authority, such as a bank, that records all transactions. Tracking the movement and location of all currency in the centralized ledger prevents double-spending because the central authority can identify and penalize someone who attempts to spend the same $10 to acquire multiple products or services. The centralized ledger decreases the ease of deception and increases the potential risk because it effectively makes it impossible for one person to give the same $10 to multiple

[10] Eric Hughes, "A Cypherpunk's Manifesto," Activism.net, Mar. 9, 1993, accessed May 30, 2019, https://www.activism.net/cypherpunk/manifesto.html.

[11] John O. McGinnis and Kyle Roche, *Bitcoin: Order Without Law in the Digital Age*, Northwestern Public Law Research Paper No. 17-06, Apr. 18, 2019, accessed May 29, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929133; and Maria Bustillos, "You Don't Understand Bitcoin Because You Think Money Is Real," *Medium*, Nov. 30, 2017, https://medium.com/s/the-crypto-collection/you-dont-understand-bitcoin-because-you-think-money-is-real-5aef45b8e952.

[12] Erik Bonadonna, "Bitcoin and the Double-Spending Problem," *Cornell University Blog for Networks II (INFO 4220)*, Mar. 29, 2013, http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/.

online vendors without incurring a penalty (e.g., an overdraft fee on a checking account). The centralized management of transactions is known as “centralized trust” or “third-party trust.”

Third-party trust

Innovators in the world of cryptocurrencies were particularly motivated to find a solution to the problem of double-spending because it is *most* likely to happen when digital currencies are exchanged: risks are lowest and deception is easiest when one person can simply create a digital copy of her money and spend it multiple times. These innovators, however, were also skeptical of using centralized ledgers to solve the problem of double-spending. Relying on a centralized ledger, they argued, simply relocates the trust.

In an ideal currency exchange, it would be impossible for buyers and sellers to cheat one another. However, because it is nearly always possible to cheat, buyers and sellers are forced to trust each other. As the financial world evolved, the risk associated with cheating decreased because, for example, more transactions occurred between strangers (who were not risking their reputations) and more transactions occurred digitally (making it easier to double-spend). Because buyers and sellers did not trust one another, they chose to place their trust in institutions instead. With a centralized ledger, a third party is trusted to secure their transaction. The use of a centralized ledger solves the problem of individuals having to trust other individuals, but it introduces the necessity of trusting the third-party authority that maintains the centralized ledger. More specifically, it requires placing trust in this third-party authority to maintain the ledger faithfully and honestly.

The birth of Bitcoin

In a 2008 paper, Satoshi Nakamoto[13] argued that relying on a centralized ledger was inherently flawed because it was a “trust-based model.”[14] Nakamoto’s paper introduced Bitcoin as a response to this problem: “an electronic payment system based on cryptographic proof instead

[13] “Satoshi Nakamoto” is a pseudonym, and the true identity of the creator (or creators) of Bitcoin remains unknown to this day. As Bitcoin advocate and entrepreneur Andreas Antonopoulos has noted: “Identity and authority are distractions from a system of mathematical proof that does not require trust. This is not a telenovela. Bitcoin is a neutral framework of trust that can bring financial empowerment to billions of people. It works because it doesn't depend on any authority. Not even Satoshi's.” Source: Chen, “Satoshi Nakamoto.”

[14] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin, 2008, https://bitcoin.org/bitcoin.pdf.

of trust…a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions."[15]

Nakamoto's solution is technologically sophisticated, but he essentially argued that the problems of double-spending and third-party trust could be solved via a decentralized and cryptographically secured digital ledger (a blockchain) in which transactions are recorded (Figure 2).

Figure 2. What is a blockchain?

*A **blockchain** is an immutable decentralized ledger:*

- *Immutable* — each new block essentially locks in previous blocks
- *Decentralized* — a peer-to-peer network of computerized contributors creates new blocks
- *Ledger* — a list (i.e., a chain) of individual records (i.e., blocks)

For more information on blockchains, see the section "Cryptocurrencies as technology."

Source: CNA.

Nakamoto's Bitcoin system relies on a ledger that is both public and secure. Because the blockchain logs all transactions, and anyone can view the blockchain, anyone can view the path of each unit of currency.[16] As a result, it is theoretically impossible to double-spend a unit of cryptocurrency (called a Bitcoin in Nakamoto's system) because everyone on the network can see whether an individual already spent that unit. Moreover, anyone participating in the network can see cryptographic work confirming that each transaction in the ledger was made by the owner of the Bitcoin in question.

Cryptocurrencies such as Bitcoin prevent double-spending because everyone who participates in the network can see every transaction—so the seller can see whether or not the buyer still

[15] Ibid.

[16] Bonadonna, "Double-Spending Problem."

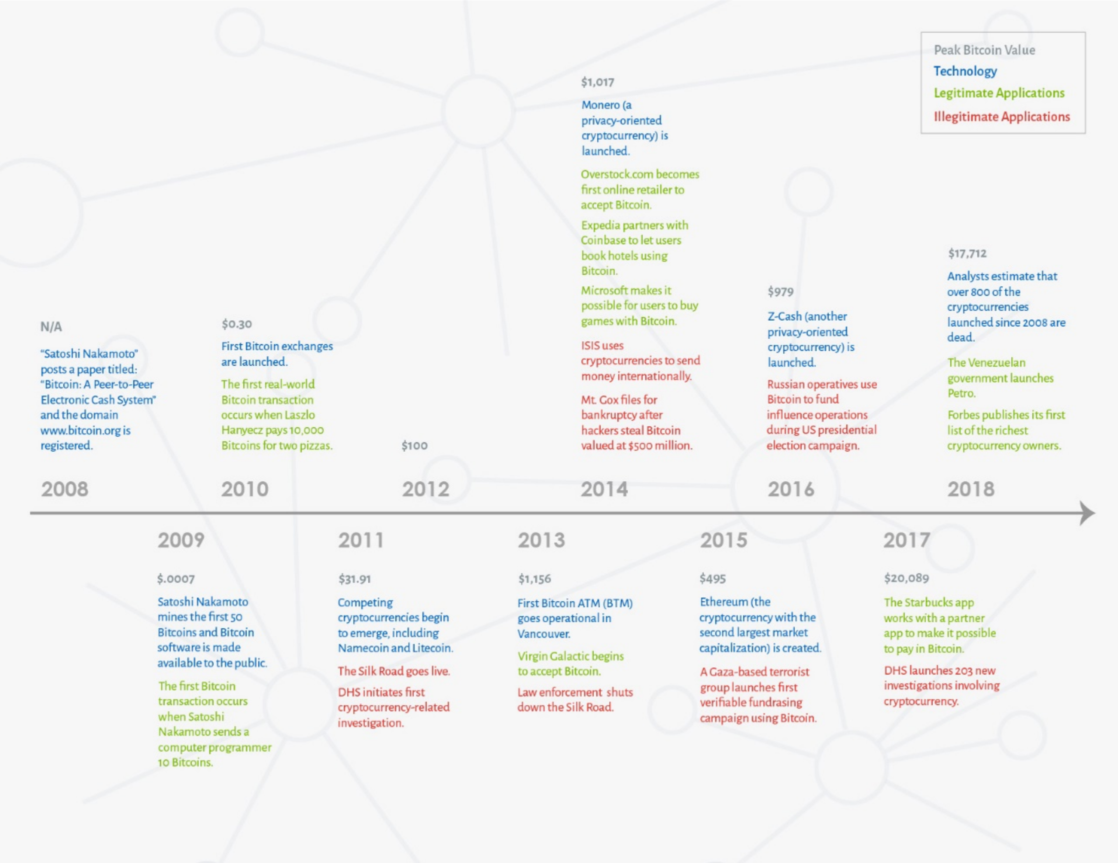
has the funds to make the purchase. Cryptocurrencies also avoid the risks associated with trusting a third-party authority such as a bank or a government because the ledger is maintained by a decentralized network that anyone can join by downloading the software.[17]

Bitcoin was not the first effort at a cryptocurrency, but Nakamoto's innovation—solving the problem of double-spending *without* relying on third-party trust—marked the beginning of viable cryptocurrencies.[18]

[17] To be clear, one can spend/trade/exchange Bitcoin without joining the Bitcoin network. Those participating in the network contribute to the maintenance of the public ledger by downloading and running a piece of software.

[18] In the early 1980s, David Chaum proposed the concept of e-cash and wrote a paper titled "Blind Signatures for Untraceable Payments." In the early 1990s, Chaum created DigiCash (which eventually went bankrupt). A few years later, Wei Dai proposed B-Money, and Nick Szabo proposed Bit Gold (both of which were theoretical online currencies with encryption-secured ledgers). Sources: Steve Fiorillo, "Bitcoin History: Timeline, Origins, and Founder," *The Street*, Aug. 17, 2018, https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578; and Bernard Marr, "A Short History of Bitcoin and Crypto Currency Everyone Should Read," *Forbes*, Dec. 6, 2017, https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/.

Figure 3. Cryptocurrency timeline



Peak Bitcoin Value

Technology

Legitimate Applications

Illegitimate Applications

2008

N/A

"Satoshi Nakamoto" posts a paper titled: "Bitcoin: A Peer-to-Peer Electronic Cash System" and the domain www.bitcoin.org is registered.

2009

$.0007

Satoshi Nakamoto mines the first 50 Bitcoins and Bitcoin software is made available to the public.

The first Bitcoin transaction occurs when Satoshi Nakamoto sends a computer programmer 10 Bitcoins.

2010

$0.30

First Bitcoin exchanges are launched.

The first real-world Bitcoin transaction occurs when Laszlo Hanyecz pays 10,000 Bitcoins for two pizzas.

2011

$31.91

Competing cryptocurrencies begin to emerge, including Namecoin and Litecoin.

The Silk Road goes live.

DHS initiates first cryptocurrency-related investigation.

2012

$100

2013

$1,156

First Bitcoin ATM (BTM) goes operational in Vancouver.

Virgin Galactic begins to accept Bitcoin.

Law enforcement shuts down the Silk Road.

2014

$1,017

Monero (a privacy-oriented cryptocurrency) is launched.

Overstock.com becomes first online retailer to accept Bitcoin.

Expedia partners with Coinbase to let users book hotels using Bitcoin.

Microsoft makes it possible for users to buy games with Bitcoin.

ISIS uses cryptocurrencies to send money internationally.

Mt. Gox files for bankruptcy after hackers steal Bitcoin valued at $500 million.

2015

$495

Ethereum (the cryptocurrency with the second largest market capitalization) is created.

A Gaza-based terrorist group launches first verifiable fundrasing campaign using Bitcoin.

2016

$979

Z-Cash (another privacy-oriented cryptocurrency) is launched.

Russian operatives use Bitcoin to fund influence operations during US presidential election campaign.

2017

$20,089

The Starbucks app works with a partner app to make it possible to pay in Bitcoin.

DHS launches 203 new investigations involving cryptocurrency.

2018

$17,712

Analysts estimate that over 800 of the cryptocurrencies launched since 2008 are dead.

The Venezuelan government launches Petro.

Forbes publishes its first list of the richest cryptocurrency owners.

Source: CNA.

How Do Cryptocurrencies Work?

The question of how cryptocurrencies work is best thought of as two distinct questions: How do cryptocurrencies work technologically? And how do cryptocurrencies work economically (i.e., as currencies)?

Cryptocurrencies as technology

The details of how cryptocurrencies work are complex, and the proliferation of cryptocurrencies over the past decade means there is no universal way to explain how they work technologically. That said, Bitcoin was the first viable cryptocurrency, and subsequent variations are largely adjustments to Bitcoin's core system. As a result, the description of how Bitcoin works that we present below is a description of the basic mechanisms common to most cryptocurrencies.

Mining

Cryptocurrencies' decentralized ledgers rely on a computerized network of users that validate transactions and protect against fraud. To verify transactions and add new blocks to the existing blockchain, computers on a cryptocurrency network (also known as "nodes") must solve complex cryptographic puzzles.

To incentivize users to dedicate computer-processing power to solve these puzzles, a Bitcoin node is rewarded with a predetermined amount of Bitcoin when it successfully does so, thereby adding a block to the blockchain. The metaphor coined for maintaining and updating the blockchain is "mining," and the nodes (known as "miners") try to solve the puzzles to create (i.e., "mine") new Bitcoin.

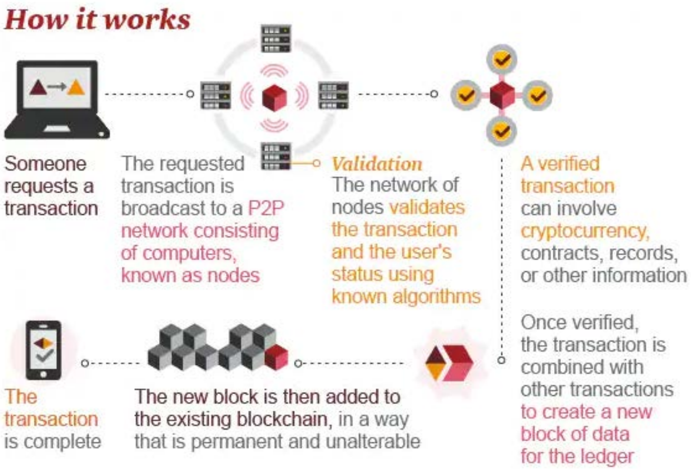
Importantly, solving the puzzle necessary to add the next block to the blockchain is more about computational power than mathematical knowledge. James Grimmelmann, a professor at Cornell Law School, tells his students that this work is closer to playing the lottery than to doing a math problem because the process essentially requires guessing random prime numbers and testing them in the puzzle.[20] The more computational power a user commits to solving the puzzle (like buying more lottery tickets), the greater chance she will be the first to solve the problem (though, as with the lottery, buying more tickets does not guarantee winning).[21]

For each cryptocurrency, all miners are users, but not all users are involved in the time-consuming and energy-intensive process of mining. Indeed, taking the example of Bitcoin, most users are not miners; the computational power necessary to solve the puzzles—and the professional operators involved in attempting to do so—makes mining from a user's home computer completely unprofitable, if not downright impossible.[22]

Transactions

So how is a new transaction validated? And how does the decentralized ledger (i.e., the blockchain) get updated? The procedure can be broken down as shown in Figure 4.

Figure 4. How a cryptocurrency transaction works


How it works
Someone requests a transaction
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes
Validation
The network of nodes validates the transaction and the user's status using known algorithms
A verified transaction can involve cryptocurrency, contracts, records, or other information
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger
The new block is then added to the existing blockchain, in a way that is permanent and unalterable
The transaction is complete

Source: "Making Sense of Bitcoin, Cryptocurrency, and Blockchain," PwC United States, accessed Mar. 20, 2019, https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.

[20] Bonadonna, "Double-Spending Problem."

[21] Rachel Withers, "Gold, Tulip Bulbs, Rai Stones?" Finding the Best Analogy for Cryptocurrencies," *Slate*, Aug. 30, 2018, https://slate.com/technology/2018/08/gold-tulip-bulbs-rai-stones-whats-the-best-analogy-for-cryptocurrency.html.

[22] "What Is Bitcoin Mining and Is It Profitable?" 99 Bitcoins, May 21, 2019, accessed May 28, 2019, https://99bitcoins.com/bitcoin-mining/.

These technical steps are more easily understood by using a real-world example, which we provide in Figure 6 on page 13. However, it is first necessary to understand the concept of public and private keys.

Figure 5. What is public key cryptography?

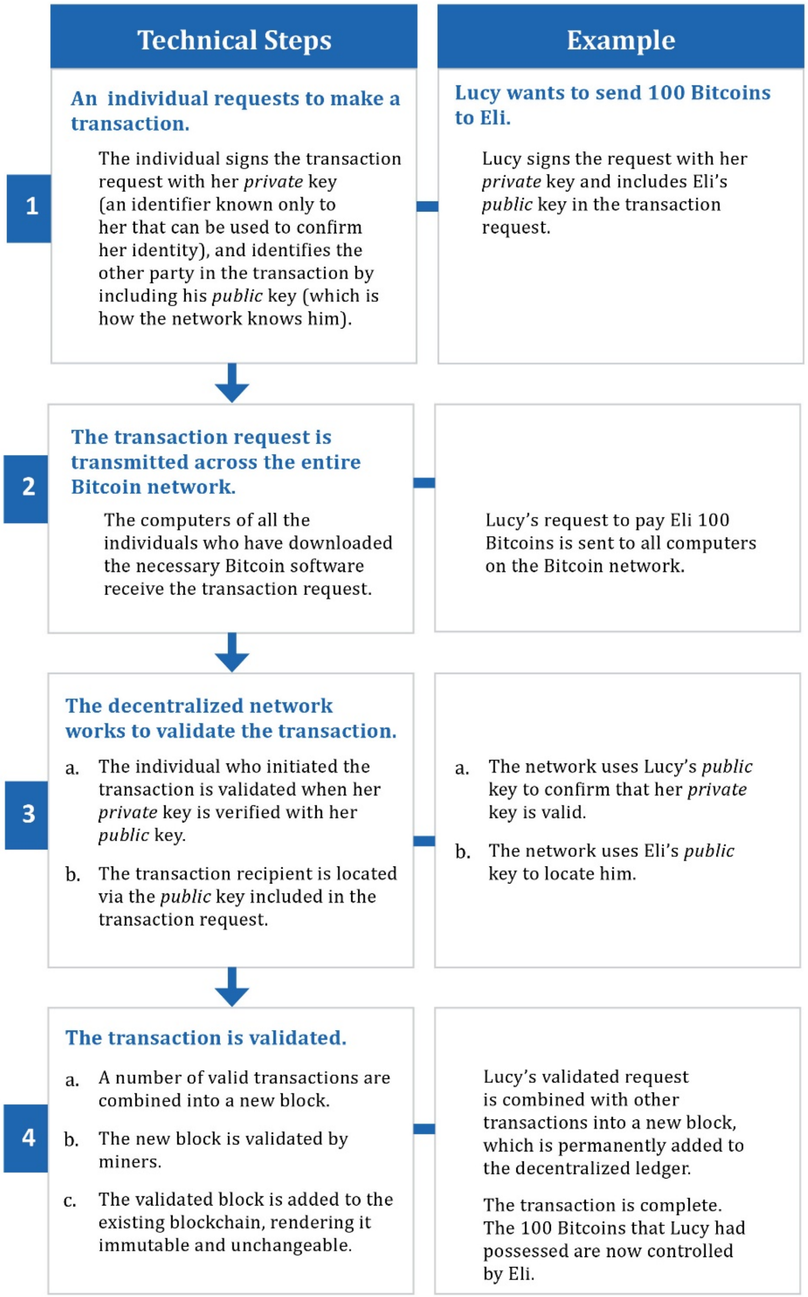
> ***Public key cryptography****—also known as asymmetric cryptography—relies on the use of different keys to encrypt and decrypt data (symmetric cryptography, by contrast, occurs when the same key is used to encrypt and decrypt data).*

Source: "Public Key Cryptography," IBM Knowledge Center, accessed Mar. 20, 2019, https://www.ibm.com/support/knowledgecenter/en/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/publickeycryptography.html.

In any financial system, it is necessary to (1) identify the recipient of the funds and (2) confirm that the transfer is legitimate. For example, a signature on a check confirms that the owner of that checking account approved the transaction. In the case of cryptocurrencies, this is done by public key cryptography, in which the private key functions as a digital signature, and works as follows.

A user shares her public key with the cryptocurrency network. When she wants to process a transaction, she "signs" the transaction request with her private key. The cryptocurrency network confirms that the request is authentic (insofar as it confirms that the user's private key was used to make the request). This process is similar to a bank comparing the signature on a check to that account holder's signature on file. Additionally, the user includes the recipient's public key in her transaction request, which tells the network where to send the funds. To complete the metaphor, the recipient's public key is the equivalent of the "To" line on a bank check.

Figure 6. Real-world example of a Bitcoin transaction



Technical Steps

Example

1

An individual requests to make a transaction.

The individual signs the transaction request with her *private* key (an identifier known only to her that can be used to confirm her identity), and identifies the other party in the transaction by including his *public* key (which is how the network knows him).

Lucy wants to send 100 Bitcoins to Eli.

Lucy signs the request with her *private* key and includes Eli's *public* key in the transaction request.

2

The transaction request is transmitted across the entire Bitcoin network.

The computers of all the individuals who have downloaded the necessary Bitcoin software receive the transaction request.

Lucy's request to pay Eli 100 Bitcoins is sent to all computers on the Bitcoin network.

3

The decentralized network works to validate the transaction.

a. The individual who initiated the transaction is validated when her *private* key is verified with her *public* key.

b. The transaction recipient is located via the *public* key included in the transaction request.

a. The network uses Lucy's *public* key to confirm that her *private* key is valid.

b. The network uses Eli's *public* key to locate him.

4

The transaction is validated.

a. A number of valid transactions are combined into a new block.

b. The new block is validated by miners.

c. The validated block is added to the existing blockchain, rendering it immutable and unchangeable.

Lucy's validated request is combined with other transactions into a new block, which is permanently added to the decentralized ledger.

The transaction is complete. The 100 Bitcoins that Lucy had possessed are now controlled by Eli.

Source: CNA.

Cryptocurrencies as currencies

The framework making cryptocurrencies function is admittedly complex, but the framework via which conventional currencies function is also complex. Although few people understand why cryptocurrencies have value, few people can explain why the green linen rectangles in their wallets have value. The major difference between cryptocurrencies and conventional currencies, for the average citizen, is that the process of spending conventional currencies (either in person or digitally) is straightforward and familiar, but the process of spending cryptocurrencies is murky and confusing.[23]

As noted at the beginning of this paper, cryptocurrency differs from most conventional currencies in five significant ways:

1. Cryptocurrencies are decentralized.
2. Cryptocurrencies rely on the blockchain instead of a centralized private ledger.
3. Cryptocurrency exchange rates can be extremely volatile, depending on supply and demand.
4. Cryptocurrencies have longer transaction times.
5. Cryptocurrency transactions are pseudonymous or anonymous.

In the previous sub-section, "Cryptocurrencies as technology," we explained the first two of these differences. With this better understanding of how cryptocurrencies work, it is now possible to consider how issues of volatility and transaction speed have impacted the adoption of cryptocurrencies for buying and selling goods and services. Below, in the "An Assessment of Cryptocurrencies: Weaknesses and Common Myths" section, we will address the critical issue of anonymity.

Volatility and transaction times

The dollar, euro, and other major conventional currencies are generally stable relative to one another. An American traveler visiting Europe for a week does not need to consider the dollar-euro exchange rate every day of his trip because the differences will be negligible. Conventional currency values are impacted by supply and demand, and they do fluctuate, but they are also moderated (and thus stabilized) by the monetary policies of central banks.

[23] The modifier "crypto" and the widespread reporting on the use of cryptocurrencies on the so-called "Dark Web" also make cryptocurrencies seem a bit illicit.

Of course, conventional currencies can—and do—undergo extreme volatility on occasion (e.g., the Venezuelan bolivar, the Iranian rial, or the Zimbabwean dollar). Generally speaking, those examples are the exception and not the rule. Moreover, these exceptional cases are also frequently the result of poor fiscal and monetary management. In other words, effective monetary policies stabilize the value of most conventional currencies (and poor monetary policies destabilize the value of conventional currencies).

Cryptocurrencies may be particularly appealing in unstable markets and under unstable governance—where populations experience volatile conventional currencies. Cryptocurrencies may be relatively stable and/or secure compared to the conventional currencies of poorly managed or underdeveloped nations.[24]

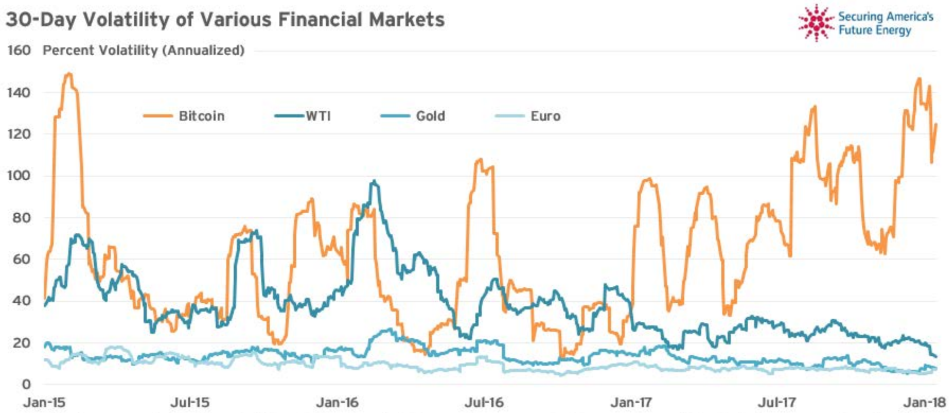
Cryptocurrencies, as we have noted, have no monetary management. They were designed, in part, to eliminate the influence of third-party authorities such as banks and governments. Although most adopters view decentralization favorably, it is a double-edged sword because no central authority regulates the swings of supply and demand. As a result, cryptocurrencies are particularly vulnerable to volatility and fluctuation—and even price manipulation.[25] Bitcoin exemplified this volatility in recent years as its value surged 1,300 percent in 2017 and then fell by more than half in May 2018.[26] Within that rise and fall, Bitcoin's value swung significantly day to day, even minute to minute, as shown in Figure 7 on the next page.

[24] Jonathan Schroden, conversation with US Army finance officer, Feb. 22, 2019.

[25] John M. Griffin and Amin Shams, "Is Bitcoin Really Un-Tethered?" June 13, 2018, https://ssrn.com/abstract=3195066 or http://dx.doi.org/10.2139/ssrn.3195066.

[26] Annie Lowry, "Bitcoin Is Falling Out of Favor on the Dark Web," *The Atlantic*, Mar. 1, 2018, https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/.

Figure 7. Volatility of bitcoin, oil, gold, and the euro, January 2015–January 2018

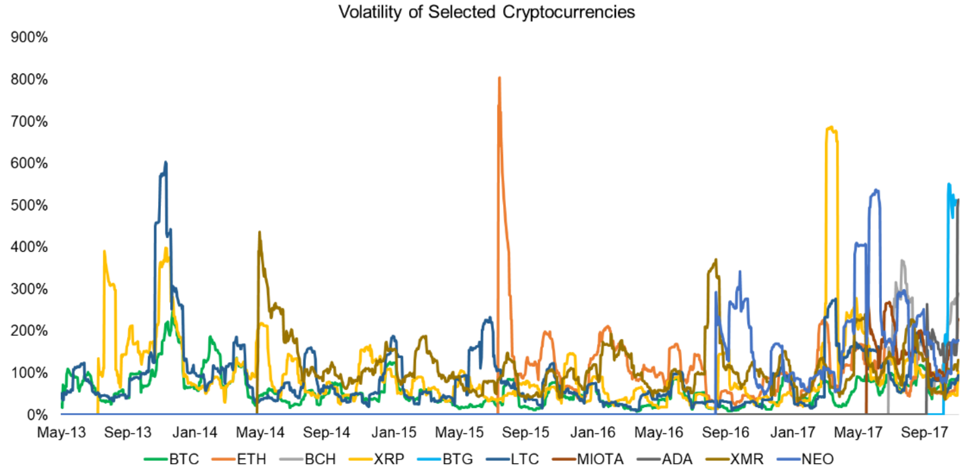


Note: All values are quoted in the U.S. dollar. Gold is shown in dollars per troy ounce. West Texas Intermediate (WTI) oil prices are shown in dollars per barrel.
Source: SAFE analysis based on data from EIA, Bloomberg, L.P., World Gold Council, and CoinDesk.com.

Source: Matt Piotrowski, "Tough Sell: Cryptocurrency Backed by Oil," Energy Fuse, Jan. 19, 2018, http://energyfuse.org/tough-sell-cryptocurrency-backed-oil/.

As the first and most popular cryptocurrency, Bitcoin's volatility is well known. However, volatility is built into the nature of cryptocurrencies, and Bitcoin is not the only—and not even the most—volatile cryptocurrency (Figure 8).

Figure 8. Volatility of 10 cryptocurrencies, May 2013–September 2017



Source: "Cryptocurrency Volatility - Friend or Foe?" *steemit*, Dec. 9, 2017, https://steemit.com/cryptocurrency/@cqr/cryptocurrency-volatility-friend-or-foe.

This instability is a significant issue for cryptocurrency users, and it is compounded by potentially long transaction times when transferring cryptocurrencies between individuals. Although one appeal of cryptocurrencies is that transactions are processed continuously, the reality is that transaction times are highly variable.[27] As noted in the above sub-section, cryptocurrency transactions are verified by nodes across the network when they solve the cryptographic puzzle required to add a block to the blockchain. However, since a transaction is not completed until it is authenticated by this network and added to the blockchain (via the work of miners), it is not an instantaneous process.

In some instances, a transaction may be processed in a few minutes (Table 1), which is only slightly more inconvenient than the near-instantaneous processing of credit cards, Venmo, or PayPal (For a comparison of transaction processing speeds, see Figure 9 on the next page).[28] However, processing Bitcoin transactions has sometimes taken days.

Table 1. Average transaction time of top five cryptocurrencies (by market capitalization), May 2018

Market Cap. Ranking	Cryptocurrency	Average Transaction Time[a]
1	Bitcoin	78 minutes
2	Ethereum	6 minutes
3	Ripple	4 seconds
4	Bitcoin Cash	60 minutes
5	EOS	1.5 seconds

Source: Sean Williams, “Ranking the Average Transaction Speeds of the 15 Largest Cryptocurrencies,” *Motley Fool*, May 23, 2018, https://www.fool.com/investing/2018/05/23/ranking-the-average-transaction-speeds-of-the-15-l.aspx.

[a] Average total time required to complete transaction, as tested in 2018.

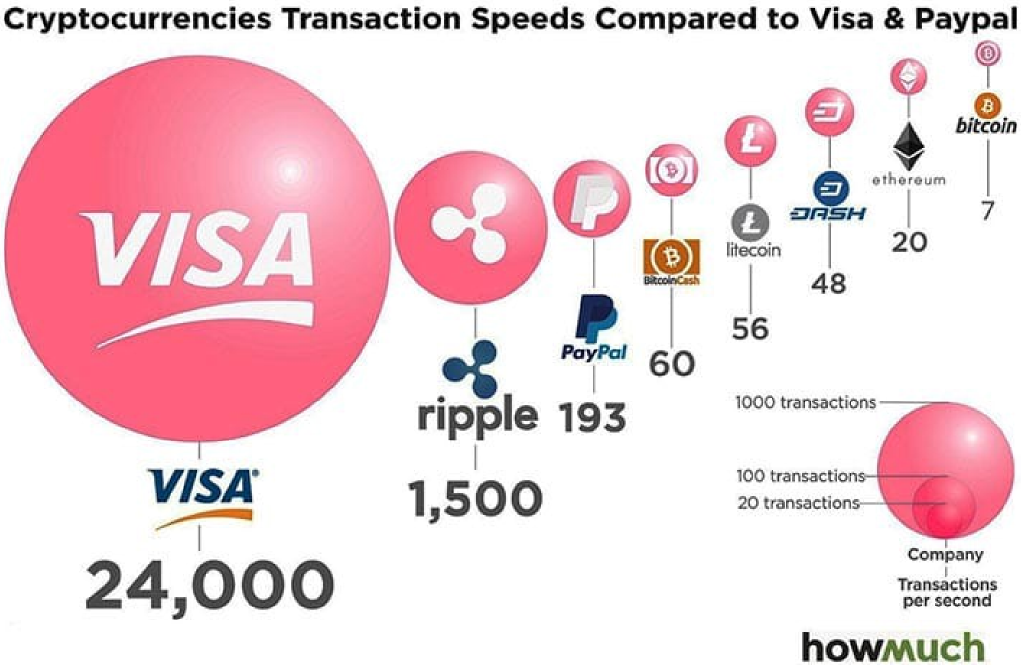
This might only be a matter of inconvenience were it not for the volatility of cryptocurrencies. Because of that volatility, lags in the processing time of a transaction could result in a currency value of much less or much greater than was intended (i.e., the exchange rate to conventional currencies might be favorable when submitting the transaction and unfavorable when the

[27] Crypto Account Builders, “The Fastest Cryptocurrency Transaction Speeds for 2018,” *Medium*, Oct. 5, 2018, https://medium.com/@johnhinkle_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-498c1baf87ef.

[28] Ibid.

transaction is finalized). For this reason, some vendors that accept cryptocurrency enforce a transaction time limit that will void purchases if not completed within a short timeframe.[29]

Figure 9. Number of transactions processed per second, October 2018



Source: Crypto Account Builders, "The Fastest Cryptocurrency Transaction Speeds for 2018," *Medium*, Oct. 5, 2018, https://medium.com/@johnhinkle_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-498c1baf87ef.

With a better understanding of how cryptocurrencies differ from conventional currencies, the question of how cryptocurrencies function as currencies is essentially the question of how to use them: How does one obtain, store, spend, and invest cryptocurrency? And how does the government approach the regulation of cryptocurrencies?

[29] As one potential solution to the problem of a cryptocurrency's value changing between the beginning and end of a transaction, the Ethereum blockchain offers "smart contracts" in which a buyer and seller can agree to the conventional currency value of a transaction. The smart contract will exchange the amount of Ethereum of that conventional currency value at the exact time of transaction completion. Source: Timothy B. Lee, "Ethereum, Explained: Why Bitcoin's Stranger Cousin Is Now Worth $1 Billion," *Vox*, May 24, 2016, https://www.vox.com/2016/5/24/11718436/ethereum-the-dao-bitcoin.

Using cryptocurrencies

Obtaining and exchanging cryptocurrencies

Although cryptocurrencies can be obtained through mining, most people simply purchase them with conventional currencies or other cryptocurrencies. These purchases can take place via exchanges, in person, or at cryptocurrency-friendly ATMs.

The most popular way to purchase cryptocurrencies is through an online exchange platform which (just like conventional currency exchanges) charges a nominal fee for the transaction. In this way, exchanging conventional currencies for cryptocurrencies (or one cryptocurrency for another) is much like exchanging dollars for euros at the bank.

The exchanges (including, but not limited to, Coinbase, Bitfinex, Bitstamp, Kraken, Gatehub, Binance, and Gemini) differ not only in the services they provide (e.g., accepting different methods of payment) and the fees they charge, but also in the user experience they offer (i.e., the degree to which the website or interface is user-friendly).[30] Coinbase is one of the most popular because it is user-friendly and provides a wallet for holding cryptocurrencies (more on that below).[31] Bitfinex is popular in part because of features similar to those found on consumer stock-trading websites.[32]

Importantly, exchanges are where most regulation of cryptocurrency takes place, so not every exchange is available from every jurisdiction.[33] The degree to which an exchange is compliant with relevant regulations influences its reputation in a complicated give-and-take. A more compliant exchange might be perceived as a safer venue through which to do business, but that compliancy undermines the promise of anonymity that many cryptocurrency users desire (for example, the exchange may collect identifying information about its users and submit

[30] Kirsten Korosec, "This Is Your Guide to Buying Bitcoin," *Fortune*, Jan. 3, 2018, http://fortune.com/2018/01/03/bitcoin-buy-how-to-cryptocurrency; and Anne Straders, "The 7 Best Cryptocurrency Exchanges in 2018," *The Street*, Nov. 27, 2018, https://www.thestreet.com/investing/bitcoin/best-7-cryptocurrency-exchanges-14777561.

[31] Steve Fiorillo, "How to Buy Bitcoin and Where," *The Street*, Apr. 9, 2018, https://www.thestreet.com/investing/bitcoin/where-to-buy-bitcoin-14549594; and Korosec, "Guide to Buying Bitcoin."

[32] Steve Fiorillo, "Selling and Trading: How to Exchange Your Bitcoins," *The Street*, Apr. 12, 2018. https://www.thestreet.com/investing/bitcoin/how-to-trade-and-sell-bitcoins-14554048.

[33] Fiorillo, "How to Buy Bitcoin."

suspicious activity reports to regulatory authorities). In short, cryptocurrency exchanges—like conventional currency exchanges—vary considerably in the degree to which they are reputable.[34]

Most cryptocurrency exchanges (like conventional currency exchanges found in airports) will require at least some form of identity confirmation and will charge at least a nominal fee. A user might aspire to avoid these requirements (to maintain anonymity and save on fees) by working outside of the system. Cryptocurrencies can also be purchased in person-to-person interactions, though such an approach is far riskier. Any travel guide will warn visitors against changing dollars for the local currency from shady characters in the local capital's shopping district, since the transaction is liable to result in scam or theft. Such a warning is equally relevant in the world of person-to-person cryptocurrency exchanges.[35] Websites such as LocalBitcoins facilitate these person-to-person exchanges by allowing buyers and sellers to find each other and arrange in-person meetings to exchange conventional currencies for cryptocurrencies.[36]

Finally, cryptocurrencies can be acquired through cryptocurrency-friendly ATMs in major cities. ATMs for Bitcoins and other cryptocurrencies (sometimes called "BTMs") have much higher transaction fees than exchanges and still require an identification process—although one *Bloomberg* report highlighted the ease of providing false identifying information—but they are nonetheless popular.[37] As of early June 2019, the website *Coin ATM Radar* maps more than 4,900 cryptocurrency ATMs worldwide for the popular currencies Bitcoin, Bitcoin Cash, Dash, Ethereum, and Litecoin.[38]

[34] Ibid.

[35] Kari Paul, "Steve Wozniak Had $70,000 in Bitcoin Stolen After Falling for a Simple, yet Perfect, Scam," *Market Watch*, Feb. 28, 2018, https://www.marketwatch.com/story/steve-wozniak-had-70000-in-bitcoin-stolen-after-falling-for-a-simple-yet-perfect-scam-2018-02-28.

[36] Dylan Dedi, "How and Where to Buy Cryptocurrency? Overview," *Cointelegraph*, Mar. 6, 2018, https://cointelegraph.com/news/how-and-where-to-buy-cryptocurrency-overview.

[37] Tom Schoenberg and Matt Robinson, "Bitcoin ATMs May Be Used to Launder Money," *Bloomberg Businessweek*, Dec. 14, 2018, https://www.bloomberg.com/features/2018-bitcoin-atm-money-laundering/.

[38] "Bitcoin ATM Map," Coin ATM Radar, accessed June 5, 2019, https://coinatmradar.com/.

Holding cryptocurrencies

Cryptocurrencies are held by their owners in *wallets* that store the public and private keys necessary to send or receive them.[39] All wallets essentially operate the same way, but they have four forms: paper wallets, hardware wallets, online or mobile wallets, and software wallets.[40] Each type of wallet differs in levels of convenience and security, with the most secure (a paper wallet) being the least convenient:

- *Paper wallets* are QR codes printed on pieces of paper. A paper wallet is secure from hackers, but if its owner loses or damages the paper, her cryptocurrency is lost—much like any cash in a real lost wallet.
- *Hardware wallets*, as the name suggests, store the owner's public and private keys on a piece of hardware (such as a USB drive) that can be unplugged from the internet and from the owner's computer.[41] Hardware wallets are more secure than online or software wallets, but they are also less convenient and cost money (most online and software wallets are free). As with a paper wallet, losing a hardware wallet (which can be as simple as forgetting the hardware in your pants pocket when washing them) means losing the cryptocurrency stored within. By contrast, "losing" an online or software private key typically occurs because someone has exploited or hacked the system.[42]
- *Online or mobile wallets* are the most convenient. However, online wallets—and phone application-based mobile wallets—involve third-party companies holding a user's private key and storing it online. Although the most reputable online wallets

[39] "Cryptocurrency Wallet Guide: A Step-by-Step Tutorial," Blockgeeks, 2017, https://blockgeeks.com/guides/cryptocurrency-wallet-guide/.

[40] Paper wallets and hardware wallets—when unplugged from an internet-enabled computer—are sometimes called "cold wallets"; whereas software, mobile, and online wallets are called "hot wallets" because they are continuously connected online. Source: "Bitcoin IRA: Hot Wallets Vs. Cold Wallets," *Bitcoin IRA*, Jan. 18, 2018, https://bitcoinira.com/articles/hot-wallets-vs-cold-wallets.

[41] Korosec, "Guide to Buying Bitcoin."

[42] Ben Dickson, "Why Bitcoin Is Struggling to Become a Mainstream Currency," *PC Magazine*, Oct. 8, 2018, https://www.pcmag.com/commentary/364184/why-bitcoin-is-struggling-to-become-a-mainstream-currency.

are rather secure, storing private keys in hackable online databases has obvious security risks.[43]

- *Software wallets* are viewed as more secure than online wallets because they run on their owners' personal computers, which can be disconnected from the internet. However, personal computers are frequently online and are consequently vulnerable to being hacked.[44] In one example, analysts created a small Bitcoin wallet on a computer and monitored to see whether anyone would attempt to steal from it. During the experiment, the bait wallet remained untouched, but its creator's wallet was hacked. As the article concluded, "If security experts can't safely keep cryptocurrencies on an internet-connected computer, nobody can."[45]

Spending cryptocurrencies

Over a thousand cryptocurrencies exist, but in reality only a handful can be used to purchase goods online or in a store. The most popular cryptocurrency for making purchases is Bitcoin, but online retailers have also started accepting other cryptocurrencies such as Ethereum, Litecoin, Dash, and Bitcoin Cash.

Proselytes of cryptocurrency have hyped announcements by large retail companies that have decided to accept Bitcoin or other cryptocurrencies as payment for their products. Overstock.com is the largest of these examples.[46] Microsoft also accepts Bitcoin for purchases in its Windows and Xbox stores.[47] Despite the excitement surrounding these announcements, very few mainstream retailers accept cryptocurrencies. Perhaps more interesting is the fact that gift cards to hundreds of retailers can be purchased with cryptocurrencies. For example, Gyft.com accepts Bitcoin as payment, and its competitor eGifter.com will take five different

[43] Fiorillo, "How to Buy Bitcoin."

[44] Ibid.

[45] Nicholas Weaver, "Inside Risks of Cryptocurrencies," *Viewpoints: Communications of the ACM* 61, no. 6 (June 2018): 3-4, https://www1.icsi.berkeley.edu/~nweaver/papers/cryptorisks.pdf.

[46] Mariam Nishanian. "8 Surprising Places Where You Can Pay with Bitcoin," *Business Insider*, Oct. 11, 2017, https://www.businessinsider.com/bitcoin-price-8-surprising-places-where-you-can-use-2017-10.

[47] Microsoft, "How to Use Bitcoin to Add Money to Your Microsoft Account," Microsoft Account Support, updated Oct. 5, 2018, https://support.microsoft.com/en-us/help/13942/microsoft-account-how-to-use-bitcoin-to-add-money-to-your-account.

cryptocurrencies.[48] So even though mainstream retailers such as Home Depot, Lowe's, Target, and Best Buy do not accept cryptocurrency payments, cryptocurrencies can be used to purchase gift cards to these stores (and many others).

As mentioned above, cryptocurrency transaction times represent a serious challenge to the widespread adoption of cryptocurrencies. At present, most retailers that "accept" cryptocurrencies do not actually accept transfers directly from customers. The transaction time of a cryptocurrency purchase would halt business at brick-and-mortar stores (imagine standing in line at the checkout counter waiting minutes, hours, or days for a blockchain transaction to be verified). The volatility of cryptocurrency values would also impact retailers and consumers, since the cost of a consumer's goods might be significantly different when that person enters the store, fills his cart, gets in line, makes the purchase, and completes the transaction.

To mitigate against these risks, such purchases are not "made" in cryptocurrencies. Instead, retailers use third parties to broker the transactions, or simply exchange the consumer's cryptocurrency for conventional currency when the transaction is processed. In this way, companies such as Coinbase, BitPay, ShapeShift, and GoCoin operate like a US-issued Visa, MasterCard, or American Express card used to purchase dinner in Europe: the credit card makes the payment in euros, these euros are exchanged for dollars at the time of the transaction, and the traveler's credit card statement reflects a dinner purchased in the corresponding dollar amount. With cryptocurrencies, the third-party vendors serve an additionally significant role in that they accept the risk that the value will go up or down before the transaction is completed on the blockchain.

Investing in cryptocurrencies

Because cryptocurrencies are not particularly practical for daily use as currencies, most people are familiar with them—and purchase them—as investments. Like those investing in the stock market, purchasers of cryptocurrencies believe that their value against conventional currencies will continue to rise.

Bitcoin exchanges have existed almost as long as the cryptocurrency itself (in 2010, Bitcoin Market and Mt. Gox established themselves as trading posts for Bitcoin).[49] These exchanges function both as moneychangers for purchasing cryptocurrencies and as online "stock

[48] Gyft, "Your Guide to Using Bitcoin with Gyft," Gyft webite, https://www.gyft.com/bitcoin/what-is-bitcoin; and eGifter, "Buy with Bitcoin at eGifter," eGifter website, https://www.egifter.com/buy-gift-cards-with-bitcoin.

[49] Fiorillo, "Bitcoin History."

markets" where the value of a cryptocurrency is measured against conventional currencies and against other cryptocurrencies. Obtaining cryptocurrencies as investments is done the same way as obtaining cryptocurrencies for purchase. An investor can get her cryptocurrency through an exchange, trade for it directly with another user, or purchase it through a BTM.

Storing cryptocurrencies remains the same no matter the intended use, though investors likely are less concerned with convenience than with security. Indeed, the security of a hardware wallet vastly outweighs the inconvenience if its user simply intends to hold onto the contents of the wallet for a long period.

Regulating cryptocurrencies

The regulatory environment surrounding cryptocurrencies is quite dynamic because the cryptocurrency ecosystem is still maturing. Keeping up with these changes in a global environment is difficult, though a number of valuable resources can be found online (e.g., "Digital Currencies: International Actions and Regulations," maintained by the international law firm Perkins Coie[50]).

At present, country-level responses to cryptocurrencies range from outright bans to government adoption. There are, however, pockets of relative consensus. Despite the use of "currency" in its name, at this date all countries that permit the use of cryptocurrencies treat these monies as "assets." As one such example, the US Internal Revenue Service (IRS) made the following determination in 2014: "For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency."[51] Because they are considered assets and not currencies for US tax purposes, making purchases with cryptocurrencies is considered the same as bartering or trading property for a service.

Although regulatory approaches vary globally, most focus on the exchanges and third-party vendors through which cryptocurrencies are purchased, stored, traded, and spent. Some of these efforts are designed to protect consumers, but most of these regulations are in place to

[50] "Digital Currencies: International Actions and Regulations," Perkins Coie, updated May 2019, accessed May 1, 2019, https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html.

[51] Keith A. Aqui, "Notice 2014-21," Internal Revenue Service, 2014, https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

ensure that cryptocurrencies are not used for money laundering, terrorist finance, or other illicit activities.

Starting in 2011, the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) began oversight of cryptocurrency exchangers, transmitters, and administrators under the Bank Secrecy Act related to anti-money laundering and combating the financing of terrorism (AML/CFT).[52] FinCEN regulates cryptocurrency exchanges operating in the United States in the same way that it regulates banks or monetary exchanges (i.e., requiring them to maintain AML/CFT activities, to keep records and reports, and to file suspicious activities with FinCEN).[53]

The Financial Action Task Force (FATF), an inter-governmental standard-setting body, recommends cryptocurrencies be regulated to counter money laundering and threat finance.[54] At the November 2018 G20 Summit, FATF called on all countries to "urgently take legal and practical steps to prevent the misuse of virtual assets."[55] The organization also updated its *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* in June 2019.[56] The European Union (EU) supports regulating cryptocurrency third-party services for

[52] Kenneth A. Blanco, "Prepared Remarks Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference," US Treasury Financial Crimes Enforcement Network, Aug. 9, 2018, https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block.

[53] Ibid.

[54] Financial Action Task Force, "Regulation of Virtual Assets," FATF website, Oct. 19, 2018, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html.

[55] Financial Action Task Force, *FATF Report to G20 Leaders' Summit,* FATF website, Nov. 2018, www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-leaders-nov-2018.html.

[56] Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF website, June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

AML/CFT purposes.[57] By 2020, all EU member states will need to extend AML/CFT rules to cryptocurrency exchanges and wallet operators.[58]

As this section illustrates, banking, consumer protection, and law enforcement authorities in individual countries have found roles in regulating the exchange of cryptocurrencies—despite the goal of cryptocurrency creators to operate their innovation outside government control. FATF's focus on cryptocurrencies suggests a positive trend in more countries implementing AML/CFT regulations on cryptocurrency exchanges.

In the next section, we explore some of the vulnerabilities of cryptocurrencies, including the issue of anonymity. Increased regulation is a positive trend, but it will be worth tracking whether users turn to so-called privacy coins (discussed below) to escape such oversight.

[57] European Securities and Markets Authority European Banking Authority, and European Insurance and Occupational Pensions Authority, "ESMA, EBA and EIOPA Warn Consumers on the Risks of Virtual Currencies," European Banking Authority, https://eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf.

[58] European Commission, "Strengthened EU Rules to Prevent Money Laundering and Fight Terrorism Financing Enter Into Force Today," European Commission, Sept. 7, 2018, accessed Apr. 29, 2019, https://ec.europa.eu/cyprus/news/20180709_2_en.

An Assessment of Cryptocurrencies: Weaknesses and Common Myths

The previous section highlighted potential advantages of cryptocurrencies over conventional currencies. In practice, not all of these advantages have been realized. Here, we explore the weaknesses of and common myths about cryptocurrencies.

Weaknesses of cryptocurrencies

Beyond the one-off theft and hacking of individual wallets, cryptocurrencies are vulnerable to threats including, but not limited to, the 51 percent problem, exchange hacking and technical vulnerabilities, and human error or avarice.

The 51 percent problem is a long-known theoretical concern that has become more pressing in recent years, since multiple such attacks have occurred. A 51 percent attack takes advantage of the fact that anyone can participate in the work of mining. In this type of an attack, a single individual or group gains control of 51 percent of the network's computing power (i.e., a single individual or group controls 51 percent of the nodes that maintain the blockchain).[59] This group then effectively controls the decentralized ledger and consequently can (a) engage in double-spending by interfering with the validation of transactions, or (b) block other nodes from mining the cryptocurrency.[60] Critically, one analyst noted that the threat was actually

[59] As noted above, mining is an energy-intensive process that is effectively cost-prohibitive to the individual user. The energy necessary to control 51 percent of a network's computing power is thus likely to be high, and so attacks are likely to occur only when the potential benefit from the attack outweighs the costs associated with launching the attack. Recent research, however, suggests that nefarious actors might *rent* the resources to launch the attack. This approach would presumably make such attacks easier to execute and more likely to happen. Source: Alyssa Hertig, "Blockchain Feared 51% Attack Now Becoming Regular," *Coindesk*, June 8, 2018, https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular.

[60] Jake Frankenfield, ed., "51% Attack," Investopedia, Feb. 7, 2019, https://www.investopedia.com/terms/1/51-attack.asp.

more significant than the name suggests and that (for technical reasons) a 51 percent attack could be orchestrated successfully with control of merely 30 percent of the network's nodes.[61]

Some research suggests that Bitcoin itself is relatively safe from a 51 percent attack, given the size of its mining network, but other cryptocurrencies (including Ethereum Classic, MonaCoin, Bitcoin Gold, ZenCash, Verge, and Litecoin Cash) have been attacked in this way over the last year.[62] Moving forward, it seems likely that such attacks will continue to occur—particularly given that this vulnerability is an inherent part of the system for most cryptocurrencies. As Litecoin founder Charlie Lee noted, "By definition, a decentralized cryptocurrency must be susceptible to 51 percent attacks."[63]

Exchange hacking and technical vulnerabilities are also serious concerns for most cryptocurrency users. In the past few years, hackers have exploited vulnerabilities in exchange platforms to steal vast numbers of private keys—in effect, stealing control of the cryptocurrencies in those wallets. Most infamously, the popular exchange Mt. Gox filed for bankruptcy in February 2014 after losing 850,000 Bitcoins (valued around $500 million at the time) in such an attack.[64]

Peer-to-peer software also is incredibly vulnerable to certain types of malware. The speed with which these malicious programs can spread across the network makes cryptocurrencies prime targets for hackers.[65] Further, malware on one cryptocurrency network could steal other types of cryptocurrencies that it encounters on a user's computer.[66] For example, a thief could deploy malware through the Bitcoin network, but steal the Ethereum or Litecoin that are also held by those Bitcoin users.

Similarly troublesome in this category are coding errors that introduce vulnerabilities into the system. One notable example comes in the form of a bug in code written by a cryptocurrency

[61] Megan McBride, conversation with industry expert, Feb. 28, 2019.

[62] Osato Avan-Nomayo, "Bitcoin 51% Attack Is Unrealistic, New Study Concludes," *Bitcoinist*, Nov. 26, 2018, https://bitcoinist.com/bitcoin-51-percent-attack-study/; and Hertig, "Blockchain 51% Attack."

[63] Gareth Jenkinson, "Ethereum Classic 51% Attack — The Reality of Proof-of-Work," *Cointelegraph*, Jan. 10, 2019, https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work.

[64] Charlie Osborne, "The Mt. Gox Bitcoin Debacle: Bankruptcy Filed, Customer Bitcoin Lost," *ZDNet*, Feb. 25, 2014, https://www.zdnet.com/article/the-mt-gox-bitcoin-debacle-bankruptcy-filed-customer-bitcoin-lost/.

[65] Weaver, "Inside Risks of Cryptocurrencies," 4.

[66] Ibid.

expert who was one of Ethereum's founders, Gavin Wood. The bug disabled access to a large number of Ethereum wallets, irreversibly freezing $150 million worth of the cryptocurrency.[67]

Human error or avarice is a universal vulnerability that is impossible to ignore. As noted above, cryptocurrencies can be permanently lost if an individual loses the paper or hardware wallet in which the cryptocurrencies are stored, but this vulnerability is compounded at the exchange level. As one example, in December 2018 the CEO of QuadrigaCX died unexpectedly and did not leave the executor of his estate (his wife) the information necessary to access his cryptocurrency wallets. As a result, the nearly $250 million in cryptocurrencies that the CEO was holding for clients became (perhaps permanently) inaccessible.[68] A still open question in the case is whether or not the CEO simply failed to ensure that this information would be passed along (i.e., human error) or staged his own death in order to steal the funds (i.e., human avarice). Although the QuadrigaCX case has a number of curious details and is still being investigated,[69] it clearly brings attention to such vulnerabilities.

Blockchain energy consumption is also a significant concern for those speculating about long-term viability. The mining system currently used to maintain the Bitcoin blockchain is effectively an increasingly costly and time-consuming guessing game. In the beginning, the puzzles were relatively simple and guessing the solutions was easy. The Bitcoin network was designed, however, to ensure that the mathematical puzzles became increasingly difficult for miners to solve. At present, the amount of processing power necessary to solve these puzzles has become prohibitive to most individual users. The power requirements alone are staggering—in early 2018, it was estimated that the Bitcoin network consumed more energy than the entire country of Ireland.[70]

[67] Ibid.

[68] Yvette Brend, "Sudden Death of Cryptocurrency Leader Sends Quadriga into Tailspin, Panicking Clients," *CBC News*, Feb. 4, 2019, https://www.cbc.ca/news/canada/british-columbia/quadriga-cryptocurrency-bitcoin-exchange-gerald-cotten-death-india-1.5002955.

[69] An investigation by Ernst & Young found that the cryptocurrencies alleged to be held by QuadrigaCX were not in the company's known wallets. See: Elizabeth Pillon and Lee Nicholson, "First Report of the Monitor," Supreme Court of Nova Scotia Hfx, No. 484742, Feb. 12, 2019, https://www.scribd.com/document/399507173/EY-QuadrigaCX-Report.

[70] Alex Hern, "Bitcoin's Energy Usage Is Huge – We Can't Afford to Ignore It," *Guardian*, Jan. 17, 2018, https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency.

Valid concerns have been raised about the growing energy demands of the Bitcoin network.[71] Importantly, though, the increase in computing power is partially a result of the number of Bitcoins awarded for adding a block and Bitcoin's recently increased value. In 2017, adding a block to the blockchain resulted in a reward of Bitcoin valued in excess of $150,000.[72] It is possible that this number will decrease, though. The network is designed to systematically reduce the number of Bitcoin rewarded for adding a block, and the value of a single Bitcoin could easily drop. More promising, engineers at universities such as MIT and Cornell, and at tech firms such as IBM and Intel, are working to identify "green blockchain innovations" that will reduce the energy consumed by the network.[73]

Common myths about cryptocurrencies

Additional practical weaknesses—and challenges for broader adoption—of cryptocurrencies derive from common misperceptions about them and the technology surrounding them.

The myth of anonymity

Above, we mentioned "anonymity" as the fifth major difference between cryptocurrencies and conventional currencies. One of the appeals of cryptocurrencies is that they allegedly allow for the anonymous transfer and movement of funds. Obviously, the in-person exchange of cash *can* also be anonymous, but *all* cryptocurrency transactions share this description. Transferring millions of dollars' worth of cryptocurrencies is also much easier than moving bulk cash.

Cryptocurrency transactions appear to be anonymous insofar as no personally identifying information is included in a transaction record. That said, cryptocurrencies are actually "pseudonymous" (not anonymous). By *pseudonymous* we mean that holders of cryptocurrencies are known by their wallet public keys (much like an author might publish under a pseudonym). Cryptocurrency transactions offer the illusion of anonymity because real

[71] And critics abound: one analyst described mining as "a competition to waste the most electricity possible by doing pointless arithmetic quintillions of times a second." Source: Hern, "Bitcoin's Energy Usage."

[72] Timothy B. Lee, "Bitcoin's Insane Energy Consumption, Explained," *ARS Technica*, Dec. 6, 2017, https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/.

[73] Helen Zhao, "Bitcoin and Blockchain Consume an Exorbitant Amount of Energy. These Engineers Are Trying to Change That," *CNBC*, Feb. 27, 2018, https://www.cnbc.com/2018/02/23/bitcoin-blockchain-consumes-a-lot-of-energy-engineers-changing-that.html.

names or other true identification are not required. However, every transaction made by every user is permanently maintained—identified by their public keys—on the blockchain. Thus, if a user's true identity is ever linked to his public key, it would be possible to trace the entirety of his engagement with the cryptocurrency (just as if an author's pen name is ever linked to her real name, all of the books she wrote under the pseudonym would be linked to her true identity).[74]

Users have deployed a number of techniques to increase their anonymity (e.g., obscuring their IP addresses or using a new public key for each transaction). Even in these cases, the public and transparent nature of the blockchain means that an incredible amount of information is available. As one example, a user might generate a new public key for each transaction, so Bitcoin transactions might be conducted via a dozen different "addresses"—much as a conventional criminal might receive funds via a dozen different post office boxes. Unlike P.O. boxes, though, the contents and records of Bitcoin accounts are public. If the user then sends these funds to someone else in a single transaction, all of the "addresses" would be publicly linked (see Figure 10 on the next page).

[74] "Bitcoin Anonymity – Is Bitcoin Anonymous?" *Buy Bitcoin Worldwide*, accessed May 2, 2019, https://www.buybitcoinworldwide.com/anonymity/; and "Is Bitcoin Anonymous?" *Bitcoin Magazine*, accessed May 2, 2019, https://bitcoinmagazine.com/guides/bitcoin-anonymous/.

Figure 10. Example of cryptocurrency transactions and social network analysis

Tracking Bitcoin transactions *– Lucy is planning to receive 10 Bitcoins from a dozen colleagues, and she has each colleague send the money to a different wallet (i.e., a different public key).*

In aggregate, Lucy now has 120 Bitcoins that she needs to send to Eli. In submitting this transfer to Eli, though, she effectively links the transactions together. An analyst tracking Lucy's online activity would become aware not only of an additional 12 public keys that she was using, but also of the 12 colleagues who sent funds to her in the first place.

Lucy's real-world identity might still be obscured at this point, but a robust understanding of her social network and activity would be emerging.

Source: CNA.

In fact, recent analysis clearly demonstrates the ways in which Bitcoin transactions can be de-anonymized. In 2018, researchers in Qatar published a paper describing how they exploited information on Bitcoin's blockchain to unmask the identities of users of hidden services such as Silk Road, The Pirate Bay, and WikiLeaks. In some cases, the researchers uncovered personally identifying information.[75] The researchers concluded, "Bitcoin addresses should always be considered exploitable."[76]

One response to the issue of pseudonymity has been the creation of so-called "privacy coins" (i.e., cryptocurrencies that prioritize privacy), which are popular with users who want more anonymity in their cryptocurrency transactions. In a cryptocurrency such as Bitcoin, the user's personal information is not shared, but her wallet and all her transactions are publicly

[75] Husam Al Jawaheri, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad, "When a Small Leak Sinks a Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis," Cornell University arXiv.org, Apr. 11, 2018, https://arxiv.org/pdf/1801.07501.pdf.

[76] Ibid.

displayed on the blockchain.[77] Privacy coins—including Zcash and Monero—mask individual transactions, which blocks a public accounting of transaction amounts and the wallets involved (though the blockchain maintains many of its core features, and thus still protects against double-spending without introducing a third-party authority).[78]

The myth of immutability

Cryptocurrency entrepreneurs and advocates highlight the immutability of the blockchain as both its defining feature and one of its most valuable qualities. However, just as a nefarious 51 percent of a network's nodes can collaborate to hijack the blockchain and steal cryptocurrency, a well-intentioned controlling majority can also manipulate the allegedly "immutable" ledger. For example, in 2016 a majority of Ethereum miners agreed to reverse a hack of their system—fixing the vulnerability a hacker exploited and "editing" the blockchain to return to its pre-hack state.[79]

The myth of a trustless system

If cryptocurrencies are not really immutable, then who has the authority to reverse the blockchain? One analyst argued that cryptocurrencies have two central authorities: the miners and the developers. Both can "manipulate" the blockchain and the rules of the cryptocurrency if they work together. Users need to trust that these two groups will not act in coherence or, if they do, that their actions will be in the greater interest.[80] Examples in which these groups do cohere to act in the greater interest abound. As mentioned in the previous paragraph, a majority of Ethereum miners collaborated to reverse a hack of their system in 2016.[81] In a May 2019 example, two groups of Bitcoin Cash miners performed what might be called a well-intentioned 51 percent attack to stop another miner from claiming Bitcoin Cash made available as the result of an update in the cryptocurrency's code.[82]

[77] Nuzzi, "ZEC: Unmatched Privacy."

[78] Ibid.; and Steve Fiorillo, "What Is Cryptocurrency? Everything You Need to Know," *The Street*, Aug. 14, 2018, https://www.thestreet.com/investing/bitcoin/what-is-cryptocurrency-14679467.

[79] Weaver, "Inside Risks of Cryptocurrencies," 5.

[80] Megan McBride, conversation with industry expert, Feb. 5, 2019.

[81] Weaver, "Inside Risks of Cryptocurrencies," 5.

[82] Max Boddy, "Two Miners Purportedly Execute 51% Attack on Bitcoin Cash Blockchain," *Cointelegraph*, May 25, 2019, https://cointelegraph.com/news/two-miners-purportedly-execute-51-attack-on-bitcoin-cash-blockchain.

Indeed, in practice, most users are neither participating in the work of maintaining the blockchain for the cryptocurrencies they own nor are they checking their transactions in the blockchain. This means that, for most users, an element of trust is still involved. However, instead of trusting a bank (which is strictly regulated), cryptocurrency users trust the anonymous nodes of a peer-to-peer network.

Cryptocurrency Issues for Policy-Makers

In our companion paper, *Cryptocurrency: Implications for Special Operations Forces*, we highlight the use of cryptocurrencies by state and non-state actors and explore the implications for US SOF. That paper enumerates attempts by nefarious actors to raise and spend cryptocurrencies for purposes such as conventional criminal activity, terrorist activity, and information operations. In addition to discussing illicit activity, the companion paper explores potential futures for the cryptocurrency ecosystem by considering the likelihood and implications of changes in adoption rates and regulation.

Some implications explored in our SOF paper will be relevant to a broader policy audience as well. Additionally, cryptocurrencies have implications for US policy-makers in the fields of investigations and law enforcement, regulation, and foreign policy. Below, we highlight five issues—three related to illicit activity and two related to the promotion of free speech and good governance—that deserve more in-depth consideration.

Challenges in countering illicit activities

A more thorough exploration of international and transnational illicit activities can be found in our companion paper. Given the breadth of such activity, there is no question that law enforcement, regulators, and private sector entities face challenges when attempting to counter illicit exploitation of the business, applications, and technology of cryptocurrencies.

Regulation gaps create safe-havens for illicit actors

As mentioned above, the regulatory environment for cryptocurrencies remains fractured. If criminals, terrorists, and other illicit actors increasingly use cryptocurrencies instead of conventional currencies, and if cryptocurrencies and their exchanges are not properly and universally regulated, challenges will grow in tracking and interdicting threat finance.[83] The

[83] Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden, "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *Joint Forces Quarterly* 92, no. 1 (2019): 58-59, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf.

lack of a coherent global approach to regulation creates cryptocurrency safe-havens if transnational criminal organizations can operate freely in countries with limited regulations.[84] Alarmingly, these illicit actors can hold and transfer their cryptocurrencies in plain sight, as long as they operate on exchanges outside the jurisdiction of countries with better oversight.[85]

The US Treasury Department already works with foreign regulators and foreign law enforcement entities to provide technical assistance and address vulnerabilities related to regulating cryptocurrency-related businesses.[86] As the international community adopts FATF standards for cryptocurrency regulations, the Treasury Department and other US and international actors should consider expanding training and assistance to build the awareness and capacity of partner countries that may be attractive to nefarious actors using cryptocurrency but are less capable of addressing the threats.

Individuals, entities, and states moving to cryptocurrency to evade sanctions

Above, we noted the challenge of illicit actors using cryptocurrencies to evade legal authorities. It is possible, however, for the authorities to be the "illicit" actors. For example, internationally sanctioned nations can use cryptocurrencies to raise money in two ways. First, governments can use national resources to purchase, mine, or steal established cryptocurrencies. For example, one private-sector intelligence company claimed North Korea mined cryptocurrencies potentially valued as high as $200 million.[87] Pyongyang's cyber army also has been behind major cryptocurrency exchange hacks. A February 2019 United Nations letter shared one estimate that North Korea stole $571 million worth of cryptocurrencies from exchanges between January 2017 and September 2018.[88]

[84] Thomas P. Ott, Testimony before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance, *Illicit Use of Virtual Currency and the Law Enforcement Response*, 115th Cong, 2nd sess. June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

[85] Megan McBride and Lauren Frey, conversation with US officials, Mar. 1, 2019.

[86] Ibid.

[87] Dudley, Pond, Roseberry, and Carden, "Evasive Maneuvers."

[88] Notes by the President, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," United Nations Security Council, Mar. 5, 2019, https://undocs.org/S/2019/171.

A second way sanctioned regimes could evade sanctions would be through establishing their own cryptocurrencies and seeking investment in these alternative currencies in exchange for conventional currencies. For example, Venezuela instituted the petro—the country's official cryptocurrency—and claimed it had received $5 billion in pledges from international donors to buy petros.[89] No evidence shows that Venezuela actually raised significant conventional currency from its petro offer.[90] However, such a scheme is one of the few methods by which a sanctioned country could raise foreign currency.[91] Currently, the potential billions raised by selling petros would still be maintained in online cryptocurrency exchanges—and therefore would not increase Venezuela's foreign currency reserves—but a more widespread adoption of cryptocurrencies in the future could potentially allow Venezuela and similarly sanctioned states to settle debts from cryptocurrency accounts instead of via central banks.

Cyberspace is adapting faster than law enforcement techniques

Although law enforcement has increased its attention to the criminal use and exploitation of cryptocurrencies, the ecosystem is evolving at a faster rate than law enforcement techniques and technologies.[92] Privacy coins are developing more advanced anonymization methods, making it harder for law enforcement to track users and transactions. Further, traditional crimes are shifting to cyberspace. For example, instead of burglaries, cyber criminals are hacking; instead of kidnapping, they are deploying ransomware. This creates a challenge for cyber divisions that are not yet resourced adequately to address these increasingly common types of crime. Further, these divisions are often not fully integrated with more established divisions, meaning they stand alone and do not always benefit from the relevant institutional expertise in other divisions.[93] That said, because criminals are not yet relying exclusively on

[89] Eric Lam, "Here's What Maduro Has Said of Venezuela's Petro Cryptocurrency," *Bloomberg*, Aug. 20, 2018, https://www.bloomberg.com/news/articles/2018-08-20/here-s-what-maduro-has-said-of-venezuela-s-petro-cryptocurrency.

[90] Ibid.

[91] Dudley, Pond, Roseberry, and Carden, "Evasive Maneuvers."

[92] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

[93] EUROPOL, "The Internet Organised Crime Threat Assessment (IOCTA)," EUROPOL website, 2015, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

cryptocurrencies to move and exchange funds, law enforcement entities can still target the transaction points where cryptocurrencies intersect with traditional financial systems.[94]

The rapid development of cybercrimes points to a need for continued training and education among law enforcement.[95] One positive development was the "Cryptocurrencies and Dark Web" training designed by the US Department of Homeland Security's Homeland Security Investigations (HSI), which is the investigations and intelligence office of the Immigration and Customs Enforcement agency. The course was a collaboration between HSI's Illicit Finance and Proceeds of Crime Unit and its Cyber Crimes Unit. By 2018, HSI conducted over 50 training sessions (nationally and internationally) for more than 4,000 law enforcement officials.[96] Those seeking to counter threats posed by cryptocurrencies must continue to expand these types of training curricula.

Opportunities for supporting free speech and good governance

The blockchain, which secures cryptocurrency transactions, has many potential applications.[97] Further exploration should be conducted on the impact a number of these applications could have on US government efforts to promote free speech and other democratic institutions—and to counter governmental corruption—globally.

Blockchain immutability can protect free speech

The US government has a track record of supporting the development of technologies to circumvent authoritarian internet censorship and monitoring.[98] Perhaps surprisingly, a cryptocurrency blockchain may be one of these technologies. In 2018, Chinese students

[94] Gregory C. Nevano, Testimony before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance, *Illicit Use of Virtual Currency and the Law Enforcement Response*, 115th Cong, 2nd sess. June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NevanoG-20180620.pdf.

[95] EUROPOL, "IOCTA."

[96] Nevano, *Illicit Use of Virtual Currency*.

[97] One such application is in the field of logistics. See: Spey, *Leveraging Blockchain*.

[98] Tor Project, "Sponsors," Tor Project website, accessed May 2, 2019, https://www.torproject.org/about/sponsors.html.en.

developed an innovative way to ensure government censors could not shut down the sharing of sensitive topics: writing statements into the metadata of cryptocurrency transactions, which would be permanently saved on the blockchain.[99] Although sharing this transaction data in-country has limits (the Chinese government could still block access to that specific transaction after it is posted), writing on the blockchain could ensure the message is not lost.[100]

By contrast, the alt-right associated Gab platform provides an example of voices outside the mainstream circumventing *industry* (not government) established limits. The platform was used by the alleged shooter at Pittsburgh's Tree of Life synagogue. Afterwards, Gab was denied access to a variety of mainstream services and it began using blockchain technology to protect its free speech outside the traditional internet.[101] As one article noted, "There are blockchain alternatives to every single service currently disabling Gab."[102] Fundraising via Paypal can be replaced by fundraising via Bitcoin; domain service via GoDaddy can be replaced by domain service via Ethereum Name Service; and webhosting via Joyent can be replaced by web hosting via Ethereum's Substratum.[103]

Potential impacts of blockchain technology on governance

Blockchain technology will change the world, or so say its advocates.[104] Even taking a skeptical view of this position, there are many efforts and potential applications to use blockchain-based solutions for governance.

[99] Spandana Singh, "Blockchain Is Helping to Circumvent Censorship in China," *Slate*, July 18, 2018, https://slate.com/technology/2018/07/blockchain-is-helping-to-circumvent-censorship-in-china.html.

[100] An important aspect of this practice that requires exploration is whether blocking access to a specific transaction would also affect that transaction's integrity, meaning it would not be verified and added to the blockchain.

[101] Michael del Castillo, "The Alt-Right's Favorite Social Network Gab's Plan to Use Blockchain to Make Itself Indestructible," *Forbes*, Oct. 31, 2018, https://www.forbes.com/sites/michaeldelcastillo/2018/10/31/the-alt-rights-favorite-social-network-gabs-plan-to-use-blockchain-to-make-itself-indestructible.

[102] Ibid.

[103] Ibid.

[104] Matthew Prewitt, "Blockchains Are Governance," *Medium*, Feb. 8, 2018, https://medium.com/blockchannel/blockchain-is-governance-e0d827b97b3f.

For example, many state agencies and private companies have used or proposed blockchain solutions to secure bureaucratic functions and to counter government corruption. Since 2012, Estonia has employed blockchain technology to secure data across sectors including health and the judiciary.[105] In 2017, the country of Georgia became the first to transfer its national land registry to the blockchain, which has reportedly shortened processing times and increased transparency in land ownership.[106] Since then, other countries—including Sweden and Brazil—have followed suit (though to varying degrees).[107] In fact, the use of blockchain to secure land registries is a topic of growing interest. A 2018 United Nations Development Program article advocated for the use of blockchain to secure land registries in India, and it outlined a proof-of-concept effort underway in the Indian city of Panchkula.[108] Transparency was also the goal of Afghanistan's interest in Bitcoin-backed bonds: the Kabul-based government hoped an auditable blockchain would address international concerns about its poor fiscal management, corruption, and threat financing.[109]

Meanwhile, companies and web-based applications such as Voatz in Boston and Moscow's Active Citizen are trying to prove that election votes can be secured via blockchain technology.[110] Advocates argue that the immutability of the blockchain, in this case verified by a closed loop of public officials and bureaucrats, would make it difficult to hack the results. A number of critics have highlighted problems with this model, since hackers could manipulate

[105] e-Estonia, *e-Estonia guide*, e-Estonia website, 2018, accessed May 29, 2019, https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf.

[106] Emmanuel Vassor, "Blockchain for Governance: Four Use Cases for Encouraging Timely Development and Adoption," *SAIS Review of International Affairs*, Jan. 16, 2019, https://www.saisreview.org/2019/01/16/blockchain-for-governance.

[107] Joseph Young, "Sweden Officially Started Using Blockchain to Register Land and Properties," *Cointelegraph*, July 6, 2017, accessed May 30, 2019, https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties.

[108] Alexandru Oprunenco and Chami Akmeemana, "Using Blockchain to Make Land Registry More Reliable in India," *United Nations Development Program Blog*, May 1, 2018, accessed May 30, 2019, https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html.

[109] Derek Tonin, "Afghanistan Considers Turning to Crypto Bonds to Rebuild," *CoinGeek*, Apr. 22, 2019, https://coingeek.com/afghanistan-considers-turning-to-crypto-bonds-to-rebuild/.

[110] Sarah Holder, "Is This Experiment in Digital Democracy Too Crazy to Work?" *Citylab*, Sept. 11, 2018, https://www.citylab.com/life/2018/09/is-this-west-virginia-experiment-in-digital-democracy-crazy/569542.

votes before they reach the blockchain.[111] Additionally the Voatz system anonymizes its users' votes—so the user would not even know if her vote was registered for the candidates she selected. Last, even though more secure elections are an ideal and could legitimize political outcomes, a blockchain verified by the government could ease the ability of that government to fake results while making it more difficult for outside polling monitors to observe voting irregularities. Clearly, more research is required to address these issues.

[111] Aaron Mak, "West Virginia Introduces Blockchain Voting App for Midterm Election," *Slate*, Sept. 25, 2018, https://slate.com/technology/2018/09/west-virginia-blockchain-voting-app-midterm-elections.html; and Holder, "Experiment in Digital Democracy."

Conclusion

Cryptocurrencies and the technologies related to them are innovative financial tools with implications for national security. As we set out to write *Cryptocurrency: Implications for Special Operations Forces*, we identified a general lack of understanding about cryptocurrencies within DOD and the US government. We hope this paper—in which we used clear, non-technical language to describe complex concepts and demystify overly technical terms—will help address that issue for policy-makers.

Inevitably, this high-level approach to describing the phenomenon of cryptocurrencies glossed over some areas cryptocurrency experts would find important[112] and left out other related matters entirely.[113] We chose to focus on the big picture to give policy-makers enough knowledge of cryptocurrencies in order to support the consideration of the opportunities and challenges cryptocurrencies present.

This paper identified cryptocurrency issues worthy of US policy-makers' consideration going forward. The national security challenges and opportunities of cryptocurrencies include safe havens for illicit actors, sanctions evasion, the speed of technological adaption, the protection of free speech, and good governance. We hope that our elucidation of the basics of cryptocurrencies—and some of the current issues surrounding them—will help the US government more effectively support legitimate cryptocurrency users and counter illicit ones.

[112] As one example, we chose to spare readers from a deep dive on cryptography and an explanation of the mathematical SHA256 hash function that miners solve to verify Bitcoin blockchain transactions. See for information on this topic: "The In's and Out's of Cryptographic Hash Functions," *Blockgeeks*, 2018, accessed May 17, 2019, https://blockgeeks.com/guides/cryptographic-hash-functions/.

[113] This report is not an investment guide. Interesting financial products are now available on commodities and futures exchanges that allow people to bet on Bitcoin and other cryptocurrencies without owning the cryptocurrencies themselves. We did not include a discussion of these markets. See, for example: "Bitcoin Futures Trading," Forex.com, accessed May 17, 2019, https://www.forex.com/en-us/education/education-themes/trading-concepts/bitcoin-futures-trading/.

Figures

Tables

Abbreviations

AML/CFT	anti-money laundering and combating the financing of terrorism
BTM	ATM for Bitcoin and/or other cryptocurrencies
DOD	US Department of Defense
EU	European Union
FATF	Financial Action Task Force
FinCEN	US Department of Treasury's Financial Crimes Enforcement Network
HSI	Homeland Security Investigations
IRS	US Internal Revenue Service
JSOU	Joint Special Operations University
SOF	special operations forces

References

Akhtar, Tanzeel. “Warming: Bitcoin Profits Are Considered Taxable Income by the IRS.” *The Street*. Dec. 5, 2017. https://www.thestreet.com/story/14411674/1/bitcoin-is-taxable.html.

Aqui, Keith A. “Notice 2014-21.” Internal Revenue Service. 2014. https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

Avan-Nomayo, Osato. “Bitcoin 51% Attack Is Unrealistic, New Study Concludes.” *Bitcoinist*. Nov. 26, 2018. https://bitcoinist.com/bitcoin-51-percent-attack-study/.

“Bitcoin Anonymity – Is Bitcoin Anonymous?” Buy Bitcoin Worldwide. Accessed May 2, 2019. https://www.buybitcoinworldwide.com/anonymity.

“Bitcoin ATM Map.” Coin ATM Radar. Accessed June 5, 2019. https://coinatmradar.com/.

“Bitcoin Futures Trading.” Forex.com. Accessed May 17, 2019. https://www.forex.com/en-us/education/education-themes/trading-concepts/bitcoin-futures-trading/.

“Bitcoin IRA: Hot Wallets Vs. Cold Wallets.” Bitcoin IRA. Jan. 18, 2018. https://bitcoinira.com/articles/hot-wallets-vs-cold-wallets.

Blanco, Kenneth A. “Prepared Remarks Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference.” US Treasury Financial Crimes Enforcement Network. Aug. 9, 2018. https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block.

Boddy, Max. “Two Miners Purportedly Execute 51% Attack on Bitcoin Cash Blockchain.” *Cointelegraph*. May 25, 2019. https://cointelegraph.com/news/two-miners-purportedly-execute-51-attack-on-bitcoin-cash-blockchain.

Bonadonna, Erik. “Bitcoin and the Double-Spending Problem.” *Cornell University Blog for Networks II (INFO 4220)*, Mar. 29, 2013. http://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/.

Brend, Yvette. “Sudden Death of Cryptocurrency Leader Sends Quadriga into Tailspin, Panicking Clients.” *CBC News*. Feb. 4, 2019. https://www.cbc.ca/news/canada/british-columbia/quadriga-cryptocurrency-bitcoin-exchange-gerald-cotten-death-india-1.5002955.

Bustillos, Maria. “You Don’t Understand Bitcoin Because You Think Money Is Real.” *Medium*. Nov. 30, 2017. https://medium.com/s/the-crypto-collection/you-dont-understand-bitcoin-because-you-think-money-is-real-5aef45b8e952.

Chen, Adrian. “We Need to Know Who Satoshi Nakamoto Is.” *New Yorker*. May 9, 2016. https://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is.

Crypto Account Builders. “The Fastest Cryptocurrency Transaction Speeds for 2018.” *Medium*. Oct. 5, 2018. https://medium.com/@johnhinkle_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-498c1baf87ef.

“Cryptocurrency Volatility—Friend or Foe?” steemit. Dec. 9, 2017. https://steemit.com/cryptocurrency/@cqr/cryptocurrency-volatility-friend-or-foe.

“Cryptocurrency Wallet Guide: A Step-by-Step Tutorial.” Blockgeeks. 2017. https://blockgeeks.com/guides/cryptocurrency-wallet-guide/.

De, Nikhilesh. “Survey: Nearly 80% of Americans Have Heard of Bitcoin.” *Coindesk*. Sept. 6, 2018. https://www.coindesk.com/survey-nearly-80-of-americans-have-heard-of-bitcoin.

Dedi, Dylan. “How and Where to Buy Cryptocurrency? Overview.” *Cointelegraph*. Mar. 6, 2018. https://cointelegraph.com/news/how-and-where-to-buy-cryptocurrency-overview.

Del Castillo, Michael. “The Alt-Right’s Favorite Social Network Gab’s Plan to Use Blockchain to Make Itself Indestructible.” *Forbes*. Oct. 31, 2018. https://www.forbes.com/sites/michaeldelcastillo/2018/10/31/the-alt-rights-favorite-social-network-gabs-plan-to-use-blockchain-to-make-itself-indestructible.

Dickson, Ben. “Why Bitcoin Is Struggling to Become a Mainstream Currency.” *PC Magazine*, Oct. 8, 2018. https://www.pcmag.com/commentary/364184/why-bitcoin-is-struggling-to-become-a-mainstream-currency.

“Digital Currencies: International Actions and Regulations.” Perkins Coie. Updated May 2019. Accessed May 1, 2019. https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html.

Dudley, Sara, Travis Pond, Ryan Roseberry, and Shawn Carden. “Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency.” *Joint Forces Quarterly* 92, no. 1 (2019): 58-59, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf.

e-Estonia. *e-Estonia guide*. e-Estonia website. 2018. Accessed May 29, 2019. https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf.

eGifter. “Buy with Bitcoin at eGifter.” eGifter website. https://www.egifter.com/buy-gift-cards-with-bitcoin.

European Commission. “Strengthened EU Rules to Prevent Money Laundering and Fight Terrorism Financing Enter Into Force Today.” European Commission. Sept. 7, 2018. Accessed Apr. 29, 2019. https://ec.europa.eu/cyprus/news/20180709_2_en.

European Securities and Markets Authority, European Banking Authority, and European Insurance and Occupational Pensions Authority. “ESMA, EBA and EIOPA Warn Consumers on the Risks of Virtual Currencies.” European Banking Authority. https://eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf.

EUROPOL. “The Internet Organised Crime Threat Assessment (IOCTA).” EUROPOL website. 2015. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

Financial Action Task Force. *FATF Report to G20 Leaders’ Summit.* FATF website. Nov. 2018. www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-leaders-nov-2018.html.

Financial Action Task Force. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF website. June 2019. https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

Financial Action Task Force. “Regulation of Virtual Assets.” FATF website. Oct. 19, 2018. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html.

Fiorillo, Steve. “Bitcoin History: Timeline, Origins, and Founder.” *The Street*. Aug. 17, 2018. https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578.

Fiorillo, Steve. “How to Buy Bitcoin and Where.” *The Street*. Apr. 9, 2018. https://www.thestreet.com/investing/bitcoin/where-to-buy-bitcoin-14549594.

Fiorillo, Steve. “Selling and Trading: How to Exchange Your Bitcoins.” *The Street*. Apr. 12, 2018. https://www.thestreet.com/investing/bitcoin/how-to-trade-and-sell-bitcoins-14554048.

Fiorillo, Steve. “What Is Cryptocurrency? Everything You Need to Know.” *The Street*. Aug. 14, 2018. https://www.thestreet.com/investing/bitcoin/what-is-cryptocurrency-14679467.

Frankel, Matthew. “What Is Bitcoin?” *Motley Fool*. Jan. 10, 2017. https://www.fool.com/retirement/2017/01/10/what-is-bitcoin-2.aspx.

Frankenfield, Jake, ed. "51% Attack." Investopedia. Feb. 7, 2019. https://www.investopedia.com/terms/1/51-attack.asp.

Griffin, John M. and Amin Shams. "Is Bitcoin Really Un-Tethered?" June 13, 2018. https://ssrn.com/abstract=3195066 or http://dx.doi.org/10.2139/ssrn.3195066.

Gyft. "Your Guide to Using Bitcoin with Gyft." Gyft website. https://www.gyft.com/bitcoin/what-is-bitcoin.

Hern, Alex. "Bitcoin's Energy Usage Is Huge – We Can't Afford to Ignore It." *Guardian*. Jan. 17, 2018. https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency.

Hertig, Alyssa. "Blockchain Feared 51% Attack Now Becoming Regular." *Coindesk*. June 8, 2018. https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular.

Holder, Sarah. "Is This Experiment in Digital Democracy Too Crazy to Work?" *Citylab.* Sept. 11, 2018. https://www.citylab.com/life/2018/09/is-this-west-virginia-experiment-in-digital-democracy-crazy/569542.

Hughes, Eric. "A Cypherpunk's Manifesto." Activism.net. Mar. 9, 1993. Accessed May 30, 2019. https://www.activism.net/cypherpunk/manifesto.html.

IBM. "Public Key Cryptography." IBM Knowledge Center. Accessed Mar. 20, 2019, https://www.ibm.com/support/knowledgecenter/en/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/publickeycryptography.html.

"The In's and Out's of Cryptographic Hash Functions." Blockgeeks. 2018. Accessed May 17, 2019. https://blockgeeks.com/guides/cryptographic-hash-functions/.

"Is Bitcoin Anonymous?" *Bitcoin Magazine*. Accessed May 2, 2019. https://bitcoinmagazine.com/guides/bitcoin-anonymous/.

Al Jawaheri, Husam, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. "When a Small Leak Sinks a Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis." Cornell University's arXiv archive. Apr. 11, 2018. https://arxiv.org/pdf/1801.07501.pdf.

Jenkinson, Gareth. "Ethereum Classic 51% Attack—The Reality of Proof-of-Work." *Cointelegraph*. Jan. 10, 2019. https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work.

Joint Special Operations University. *Special Operations Research Topics 2018 (Revised Edition for Academic Year 2019).* MacDill AFB FL: JSOU Press, 2018. https://jsou.libguides.com/ld.php?content_id=41898487.

Korosec, Kirsten. “This Is Your Guide to Buying Bitcoin.” *Fortune*. Jan. 3, 2018. http://fortune.com/2018/01/03/bitcoin-buy-how-to-cryptocurrency.

Lam, Eric. “Here’s What Maduro Has Said of Venezuela’s Petro Cryptocurrency.” *Bloomberg*. Aug. 20, 2018. https://www.bloomberg.com/news/articles/2018-08-20/here-s-what-maduro-has-said-of-venezuela-s-petro-cryptocurrency.

Lee, Timothy B. “Bitcoin’s Insane Energy Consumption, Explained.” *ARS Technica*. Dec. 6, 2017. https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/.

Lee, Timothy B. “Ethereum, Explained: Why Bitcoin's Stranger Cousin Is Now Worth $1 Billion.” *Vox*. May 24, 2016. https://www.vox.com/2016/5/24/11718436/ethereum-the-dao-bitcoin.

Lowry, Annie. “Bitcoin Is Falling Out of Favor on the Dark Web.” *Atlantic*. Mar. 1, 2018. https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/.

Mak, Aaron. “West Virginia Introduces Blockchain Voting App for Midterm Election.” *Slate*. Sept. 25, 2018. https://slate.com/technology/2018/09/west-virginia-blockchain-voting-app-midterm-elections.html.

Marr, Bernard. “A Short History of Bitcoin and Crypto Currency Everyone Should Read.” *Forbes*. Dec. 6, 2017. https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/.

McBride, Megan, conversation with industry expert, Feb. 5, 2019.

McBride, Megan, conversation with industry expert, Feb. 28, 2019.

McBride, Megan and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

McBride, Megan and Lauren Frey, conversation with US officials, Mar. 1, 2019.

McGinnis, John O. and Kyle Roche. *Bitcoin: Order Without Law in the Digital Age*. Northwestern Public Law Research Paper No. 17-06. Apr. 18, 2019. Accessed May 29, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929133.

Merriam-Webster. "Cryptocurrency." Merriam-Webster website. Accessed May 2, 2019. https://www.merriam-webster.com/dictionary/cryptocurrency.

Microsoft. “How to Use Bitcoin to Add Money to Your Microsoft Account.” Microsoft Account Support. Updated Oct. 5, 2018. https://support.microsoft.com/en-us/help/13942/microsoft-account-how-to-use-bitcoin-to-add-money-to-your-account.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin. 2008. https://bitcoin.org/bitcoin.pdf.

Nevano, Gregory C. Testimony before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance. *Illicit Use of Virtual Currency and the Law Enforcement Response*. 115th Cong, 2nd sess. June 20, 2018. https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NevanoG-20180620.pdf.

Nishanian, Mariam. "8 Surprising Places Where You Can Pay with Bitcoin." *Business Insider*. Oct. 11, 2017. https://www.businessinsider.com/bitcoin-price-8-surprising-places-where-you-can-use-2017-10.

Notes by the President. "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)." United Nations Security Council. Mar. 5, 2019. https://undocs.org/S/2019/171.

Nuzzi, Lucas. "ZEC: Unmatched Privacy in a Public Blockchain." *Medium*. Sept. 17, 2018. https://medium.com/digitalassetresearch/zec-best-in-class-privacy-in-a-public-blockchain-1df2a3728739.

Oprunenco, Alexandru and Chami Akmeemana. "Using Blockchain to Make Land Registry More Reliable in India." United Nations Development Program Blog. May 1, 2018. Accessed May 30, 2019. https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html.

Osborne, Charlie. "The Mt. Gox Bitcoin Debacle: Bankruptcy Filed, Customer Bitcoin Lost." *ZDNet*. Feb. 25, 2014. https://www.zdnet.com/article/the-mt-gox-bitcoin-debacle-bankruptcy-filed-customer-bitcoin-lost/.

Ott, Thomas P. Testimony before the House Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance. *Illicit Use of Virtual Currency and the Law Enforcement Response*. 115th Cong, 2nd sess. June 20, 2018. https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

Paul, Kari. "Steve Wozniak Had $70,000 in Bitcoin Stolen After Falling for a Simple, yet Perfect, Scam." *Market Watch*. Feb. 28, 2018. https://www.marketwatch.com/story/steve-wozniak-had-70000-in-bitcoin-stolen-after-falling-for-a-simple-yet-perfect-scam-2018-02-28.

Pillon, Elizabeth and Lee Nicholson. "First Report of the Monitor." Supreme Court of Nova Scotia Hfx. No. 484742. Feb. 12, 2019. Available at https://www.scribd.com/document/399507173/EY-QuadrigaCX-Report.

Piotrowski, Matt. "Tough Sell: Cryptocurrency Backed by Oil." Energy Fuse. Jan. 19, 2018. http://energyfuse.org/tough-sell-cryptocurrency-backed-oil/.

Prewitt, Matthew. "Blockchains Are Governance." *Medium*. Feb. 8, 2018. https://medium.com/blockchannel/blockchain-is-governance-e0d827b97b3f.

PwC. "Making Sense of Bitcoin, Cryptocurrency, and Blockchain." PwC United States. Accessed Mar. 20, 2019. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.

Schoenberg, Tom and Matt Robinson. "Bitcoin ATMs May Be Used to Launder Money." *Bloomberg Businessweek*. Dec. 14, 2018. https://www.bloomberg.com/features/2018-bitcoin-atm-money-laundering/.

Schroden, Jonathan, conversation with US Army finance officer, Feb. 22, 2019.

Singh, Spandana. "Blockchain Is Helping to Circumvent Censorship in China." *Slate*. July 18, 2018. https://slate.com/technology/2018/07/blockchain-is-helping-to-circumvent-censorship-in-china.html.

Spey, S. John. *Leveraging Blockchain to Secure Logistics Information*. CNA. 2018. DOP-2018-U-018289-Final.

Stead, Chris. "Bitcoin 101: What Is It and Why Does It Matter?" *IGN.* Jan. 17, 2018. https://www.ign.com/articles/2018/01/17/bitcoin-101-what-is-it-and-why-does-it-matter.

Straders, Anne. "The 7 Best Cryptocurrency Exchanges in 2018." *The Street*. Nov. 27, 2018. https://www.thestreet.com/investing/bitcoin/best-7-cryptocurrency-exchanges-14777561.

Tonin, Derek. "Afghanistan Considers Turning to Crypto Bonds to Rebuild." *CoinGeek*. Apr. 22, 2019. https://coingeek.com/afghanistan-considers-turning-to-crypto-bonds-to-rebuild/.

Tor Project. "Sponsors." Tor Project website. Accessed May 2, 2019. https://www.torproject.org/about/sponsors.html.en.

Vassor, Emmanuel. "Blockchain for Governance: Four Use Cases for Encouraging Timely Development and Adoption." *SAIS Review of International Affairs*. Jan. 16, 2019. https://www.saisreview.org/2019/01/16/blockchain-for-governance.

Weaver, Nicholas. "Inside Risks of Cryptocurrencies." *Viewpoints: Communications of the ACM* 61, no. 6 (June 2018). https://www1.icsi.berkeley.edu/~nweaver/papers/cryptorisks.pdf.

"What Is Bitcoin Mining and Is It Profitable?" 99 Bitcoins. May 21, 2019. Accessed May 28, 2019. https://99bitcoins.com/bitcoin-mining/.

Williams, Sean. "Ranking the Average Transaction Speeds of the 15 Largest Cryptocurrencies." *Motley Fool.* May 23, 2018. https://www.fool.com/investing/2018/05/23/ranking-the-average-transaction-speeds-of-the-15-l.aspx.

Withers, Rachel. "Gold, Tulip Bulbs, Rai Stones?: Finding the Best Analogy for Cryptocurrencies." *Slate*. Aug. 30, 2018. https://slate.com/technology/2018/08/gold-tulip-bulbs-rai-stones-whats-the-best-analogy-for-cryptocurrency.html.

Young, Joseph. "Sweden Officially Started Using Blockchain to Register Land and Properties." *Cointelegraph*. July 6, 2017. Accessed May 30, 2019. https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties.

Zhao, Helen. "Bitcoin and Blockchain Consume an Exorbitant Amount of Energy. These Engineers Are Trying to Change That." *CNBC*. Feb. 27, 2018. https://www.cnbc.com/2018/02/23/bitcoin-blockchain-consumes-a-lot-of-energy-engineers-changing-that.html.

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

CNA
ANALYSIS & SOLUTIONS

3003 Washington Boulevard, Arlington, VA 22201

www.cna.org ● 703-824-2000